第 1 章

智能运维概述

智能运维（Artificial Intelligence for IT Operations，AIOps）作为一种新兴的运维模式，它通过机器学习、深度学习等人工智能技术对 IT 系统进行自动化监控、故障诊断和性能优化。它能够实时分析海量多模态运维数据，自动识别异常、定位故障根因并提供解决方案，相比传统基于规则和脚本的运维方式具有更强的自适应能力和泛化性。AIOps 不仅能显著提升运维效率，降低人力成本，还能通过预测性维护有效预防系统故障，现已成为保障微服务等复杂分布式系统稳定运行的关键技术。本章将介绍智能运维的兴起、发展历程、技术基础，以及智能运维的应用和现有标准。

1.1 引言

1.1.1 智能运维的兴起

在数字化时代的浪潮下，随着信息技术的迅猛发展，企业的 IT 基础设施和应用系统变得愈加庞大和复杂。在传统模式下，运维工作主要依赖人工操作和经验积累，面对系统的复杂性和快速变化，运维人员需要投入大量时间和精力来进行故障排查、性能调优和系统维护。这种方式不仅效率低下，而且容易受到人为因素的影响，难以

保障系统的稳定性和高可用性。以下是传统运维面临的一些主要挑战：

（1）系统复杂性。现代企业的 IT 环境包括多种系统、应用、服务和设备，这些系统往往具有复杂的依赖关系。传统运维方法在应对这种复杂性时显得力不从心，故障排查和系统维护变得烦琐且耗时。

（2）数据爆炸。数据量的急剧增加使得传统的监控和管理工具难以有效处理。大量的日志、性能数据和事件信息使得人工筛查和分析变得不可行。

（3）运维效率低。传统运维依赖人工操作和经验积累，运维人员需要进行繁重的手工配置和故障处理。这种模式不仅效率低，而且容易出错，难以应对快速变化的业务需求。

（4）故障响应滞后。传统运维模式通常在故障发生后才进行响应，导致系统的恢复时间较长。预防性维护和故障预测能力不足，可能会导致系统的长期不稳定运行。

（5）人工干预多。传统运维大量依赖人工干预，容易受到人为错误的影响。运维人员需要处理大量的告警和问题，这不仅耗费时间，而且可能影响其他重要任务的执行。

因此，智能运维应运而生，旨在通过自动化和智能化手段，提升运维工作的效率和效果。智能运维借助机器学习、深度学习、自然语言处理和大数据分析等先进的技术手段，致力于提升运维管理的智能化水平。这些技术提供了更强大的数据处理能力和智能分析算法，使得运维管理能够从被动响应转变为主动预测和自动修复。智能运维不仅能够提供实时监控、智能分析和自动化修复，满足企业对高效运维的需求，还能显著降低运维成本和复杂性，实现对 IT 资源的优化管理。

根据我国“十四五”规划和 2035 年远景目标纲要，支持具备条件的大型企业建立一体化数字平台，推动全流程数据的无缝贯通，形成基于数据的智能决策能力，以提升企业整体运营效率。在规划中明确提到智能运维作为关键技术的重要性，这表明智能运维正成为行业发展的必然趋势。

1.1.2 智能运维的发展历程

智能运维的发展可以追溯到信息技术发展的早期阶段。最初，运维工作主要依赖手工操作和定期检查，技术水平和自动化程度相对较低。随着计算机技术的发展，运维工具和技术逐渐引入了自动化脚本和监控系统，但依然主要依赖人工干预和管理。

进入 21 世纪，随着大数据、云计算、人工智能等技术的迅猛发展，运维领域开始出现新的变革。智能运维的概念逐渐得到重视，并在实际应用中取得了显著成效。具体的发展历程可以分为以下几个阶段：

（1）基础监控阶段。这一阶段的运维工作主要依赖基础的监控系统和告警机制。监控系统通过收集系统的性能数据、日志信息等，及时发现异常并触发告警。然而，这一阶段的监控系统仍然存在一定的局限性，例如告警信息冗余过多、误报率高，导致运维人员需要花费大量时间进行筛选和处理。

（2）自动化运维阶段。随着自动化技术的发展，运维工作开始引入自动化工具和脚本。自动化运维可以实现对常见故障的自动修复和处理，提高了运维效率。然而，这一阶段的自动化程度仍然有限，对于复杂问题的处理仍然需要依赖人工干预。

（3）智能化运维阶段。进入智能化运维阶段，运维工作开始引入机器学习、深度学习等人工智能技术，通过对大量数据的分析和建模，预测和预防潜在问题，实现更加智能和自动化的运维管理。这一阶段的智能运维系统不仅能够实时监控系统状态，还可以通过智能算法进行问题预测和自动修复，大幅提升了系统的可靠性和运维效率。

1.1.3　智能运维的技术基础

智能运维的实现依赖多种先进技术的支持，主要包括以下几个方面：

（1）大数据分析。智能运维系统通过对大量运维数据的收集和分析，识别系统的性能瓶颈和潜在风险。大数据分析技术能够从海量数据中提取有价值的信息，帮助运维人员做出更加准确的决策。

（2）人工智能。人工智能技术在智能运维中扮演着重要角色。通过机器学习和深度学习算法，智能运维系统能够自动识别和预测系统故障，优化资源配置，并进行智能化的故障处理。

（3）自动化工具。自动化工具的应用使得运维工作能够实现自动化执行，减少人工干预。自动化工具包括自动化运维平台、配置管理工具、自动化测试工具等，能够有效提高运维效率和准确性。

（4）自然语言处理。自然语言处理技术使得智能运维系统能够理解和处理运维人员的自然语言输入，提供智能化的故障诊断和处理建议，提高运维工作的便捷性。

1.1.4 智能运维的目标

智能运维将传统运维与先进的技术结合起来，通过智能化手段提升运维管理的自动化、精准度和效率。其主要目标包括以下几个方面：

（1）自动化与智能化。通过引入自动化工具和智能算法，减少人工干预，实现运维任务的自动化执行，提升工作效率和准确性。

（2）数据驱动决策。利用大数据分析和人工智能技术，从海量运维数据中提取有价值的信息，支持精准的决策和优化建议。

（3）实时监控与预警。通过实时监控系统状态和性能指标，及时发现潜在问题和异常，提前预警并进行自动化处理，确保系统的高可用性和稳定性。

（4）故障预测与预防。通过机器学习算法分析历史数据，预测潜在故障和风险，采取预防措施，减少故障发生频率和系统停机时间。

1.2 智能运维的应用

1.2.1 智能运维的应用领域

智能运维在多个行业和领域中展现出了广泛的应用潜力，主要包括以下几个方面。

（1）数据中心运维：在数据中心，智能运维系统可以实时监控服务器、网络设备和存储设备的状态，自动检测和修复故障，优化资源利用率，降低运维成本。

（2）云计算平台：在云计算环境中，智能运维可以实现对虚拟机、容器和应用程序的智能化管理，提高系统的可靠性和性能。通过智能调度和自动扩展，云计算平台能够应对动态的负载变化。

（3）金融行业：在金融行业，智能运维系统可以通过实时监控和数据分析，预防和应对系统故障，保障金融交易的稳定性和安全性。此外，智能运维还可以帮助金融机构进行风险管理和合规检查。

（4）电信行业：在电信行业，智能运维可以实现对网络设备和通信系统的智能化管理，提高网络的可靠性和服务质量。通过智能化的故障诊断和修复，减少服务中断时间。

（5）制造业：在制造业中，智能运维系统可以通过对生产设备和生产线的实时监控，预测设备故障，优化生产流程，提高生产效率和产品质量。

随着技术的不断发展和应用的深入，智能运维将继续发挥重要作用，更加智能化、自动化，能够更好地应对复杂的 IT 环境和业务需求。通过持续创新和技术迭代，智能运维有望为企业提供更加高效、可靠的运维解决方案，助力企业在数字化时代的成功转型。

1.2.2　智能运维要解决的问题

智能运维是现代企业为应对复杂IT环境和提升运维效率而采用的先进运维模式。它通过自动化、人工智能、大数据分析等技术手段，旨在解决传统运维模式中的一系列问题。以下是智能运维需要解决的主要问题及其对应的解决策略。

1. 系统复杂性管理

现代 IT 环境通常包括多种系统、应用、服务和设备，这些系统之间具有复杂的依赖关系。传统运维方法在面对这种复杂性时，往往显得力不从心。系统的复杂性使得故障排查、性能优化和维护管理变得异常困难。

智能运维通过集成和分析多源数据，能够自动识别系统间的复杂依赖关系和潜在的故障点。此外，采用自动化监控和告警系统，实时跟踪系统状态，及时发现和处理潜在问题，从而简化复杂环境的管理。

2. 大数据处理和分析

IT 系统生成的数据量巨大，包括日志、性能指标、告警信息等。传统的运维方法难以有效处理和分析这些海量数据。数据的冗余和噪声往往导致信息过载，使得有用信息难以提取和利用。

智能运维采用大数据处理和分析技术，对海量数据进行有效管理。通过数据清洗、集成和存储，利用机器学习和数据挖掘技术分析历史数据，发现数据中的模式和趋势，从而实现精准的故障预测、性能优化和资源调度。

3. 运维效率和自动化

传统运维往往依赖人工操作和经验积累，导致运维效率低下。重复性任务和故障处理过程烦琐，人工干预多，容易出错且耗时。

自动化工具可以执行日常运维任务，如系统配置、更新、故障处理等，减少人工操作和干预。自动化脚本和运维平台能够进行批量操作和任务调度，提高工作效率。智能运维系统能够实现自动化的故障修复，通过智能算法快速处理和解决常见问题，降低运维人员的工作负担。

4. 故障预测与预防

传统运维模式通常在故障发生后才进行响应，导致系统恢复时间较长。预防性维护和故障预测能力不足，难以避免系统长期不稳定。

智能运维对系统数据进行深入分析，识别潜在的故障模式和风险。通过建立预测模型能够提前预警，采取预防性措施，以避免故障的发生，从而实现更加主动的运维管理。

5. 运维决策支持

传统运维决策往往依赖人工经验和直觉，缺乏科学的数据支持。这种决策方式可能导致决策不准确，影响系统性能和业务连续性。

智能运维通过数据驱动的决策支持系统，可以为运维团队提供科学的决策依据。通过整合和分析各类数据，生成可操作的见解和建议。

6. 资源优化和管理

IT 资源的管理和优化是传统运维中的一个重要问题。资源配置不当可能导致资源浪费或不足，影响系统性能和业务运营。

智能运维通过实时数据分析，动态调整资源，根据负载变化自动扩展或缩减计算资源，优化资源利用率。它还可以通过预测分析，提前规划资源需求，避免资源短缺或过度配置的问题。

1.3 智能运维的相关标准

标准化是通过达成对某项技术的共识，制定和实施技术标准的过程。这一过程有助于保障服务或产品质量，建立统一认知，提高技术的通用性和互操作性，并减少不必要的多样性。目前，已有研究尝试通过标准化来解决人工智能领域的统一术语和技

术规格问题，以及技术在特定应用场景中的适配难题。因此，制定智能运维标准是一种有效的解决方案，可以帮助从业人员了解智能运维的基本知识，掌握实践要点，识别和改进现有的不足，从而提升智能运维的实际效果。标准化为不同背景下的智能运维实践提供了必要条件，对提高整个行业的智能运维能力至关重要。

1.3.1　运维相关的现有标准

在国内，信息技术相关的国家标准和行业标准的制定工作由信息技术服务标准体系（IT Service Standard，ITSS）主导。在运维领域，ITSS 4.0+框架中的国家标准 GB/T 28827.1《信息技术服务 运行维护 第 1 部分：通用要求》仍然是市场的主要标准。该标准围绕人员、过程、技术和资源 4 个关键能力要素，提出了具体的要求和评价指标，建立了一个“策划-实施-检查-改进”的能力管理体系，指导主要运维企业构建运行维护服务能力。

在 GB/T 28827.1 通用要求的基础上，相关的国家标准 GB/T 28827.2~6 对具体的运行维护工作进行了详细规范，包括交付、应急响应、数据中心服务和应用系统服务等方面。此外，ITSS 的内部标准基于这些国家标准，提供了运维能力服务成熟度的评估标准。

国家标准 GB/T 33136 借鉴了 CMMI（Capability Maturity Model Integration，能力成熟度模型集成）和 COBIT（Control Objectives for Information and related Technology，信息系统和技术控制目标）等模型，提出了数据中心运维服务能力成熟度的标准，涵盖 33 个数据中心管理能力项的关键活动，并提供了 5 个等级的服务能力成熟度评级。国家标准 GB/T 38633 则针对大数据系统的运维和管理，提出了具体的要求，包括安装部署、监控告警和服务管理等多个方面的运维活动。

国际标准化组织发布的 ISO 20000 系列是公认的 IT 服务运维管理标准，共包括 7 个部分：

- ISO 20000-1 定义了 IT 服务运维管理系统的功能需求及相关要求。
- ISO 20000-2 对 ISO 20000-1 的要求进行了详细解释。
- ISO 20000-3 和 ISO 20000-5 提供了实现和使用 ISO 20000-1 系统的建议。
- ISO 20000-6 补充了认证和审计需求。
- ISO 20000-11 和 ISO 20000-12 将 ISO 20000-1 的要求与 ITIL（Information Technology Infrastructure Library，信息技术基础设施库）和 CMMI-SVC

（Capability Maturity Model Integration for Services，服务能力成熟度模型集成）中的实践对齐。

- ISO 20000-10 整理了标准系列的构成和术语定义。
- 此外，ISO 33054 列出了 IT 服务运维系统的 33 个使用场景的过程模型，并与 ISO 20000-1 中的功能点对接；ISO 33074 则依据 ISO 33004 建立了这些过程模型的评估标准。

类似地，欧洲电信标准化协会（European Telecommunications Standards Institute，ETSI）也推出了两个标准：

- ETSI GS NFV-MAN 001 针对网络功能虚拟化（Network Functions Virtualization，NFV）提出了详细的功能需求。
- ETSI TS 128 530 针对 5G 网络中的具体场景（如网元管理、基础设施管理和网络切片管理）提出了详细的功能需求。

在此基础上，ETSI 创建了新的标准系列 ETSI ZSM，旨在实现自动化网络运维：

- ETSI GS ZSM-001 定义了自动化网络运维的功能要求。
- ETSI GS ZSM-002 定义了自动化网络运维的参考架构。
- ETSI GS ZSM-007 提供了相关术语和定义的整理。

国际电信联盟（International Telecommunication Union，ITU）的运维标准主要集中在通信管理网（Telecommunication Management Network，TMN）上：

- ITU-T M.3010 定义了 TMN 的目标、功能模块和结构。
- ITU-T M.3400 在性能、故障、配置、审计和安全方面提出了具体要求。
- ITU-T M.3070 针对云架构系统的产品、服务和资源管理给出了功能要求。
- ITU-T M.3040 旨在实现自动化运维，提出了线上巡检和服务激活等场景的功能模块和自动化流程。
- ITU-T M.3041 进一步推出了 SOMM（Smart Operation, Management and Maintenance）框架，将 TMN 的自动化运维功能分为场景应用、管理服务、数据管理和基础设施管理 4 个层级。

上述运维标准主要针对传统的人工 IT 运维，提出了功能性和流程性要求，并对自动化运维能力也有所涉及。大多数能够实施智能运维的企业通常已满足这些标准的要求，甚至获得了相关认证。然而，对于无法满足这些标准的企业，其运维数据治理

能力可能无法支持人工智能技术。这些企业应当遵循“传统运维→自动化运维→智能运维”的实施路径，首先致力于满足基本的 IT 运维标准，然后逐步建设智能运维能力。

1.3.2　人工智能的现有标准

ISO（International Organization for Standardization，国际标准化组织）于 2021 年发布了更新的人工智能概念和术语定义标准——ISO 22989，该标准将人工智能术语分为人工智能、机器学习、神经网络、可信性和自然语言处理 5 个部分进行定义。相较于旧版，ISO 22989 涵盖近年来主流的人工智能算法和模型，如卷积神经网络（Convolutional Neural Network，CNN）、长短期记忆网络（Long Short-Term Memory，LSTM）和迁移学习（Transfer Learning），并对强 AI 与弱 AI、符号与非符号方法、AI 系统生命周期及生态等常见概念进行了解释。

ISO 的人工智能系统标准 ISO 23053 将系统划分为 3 个部分：模型开发与使用、软件工具与技术以及输入数据，并在此基础上定义了机器学习流水线（ML Pipeline），描述了在人工智能系统中开发、部署和运行机器学习模型的过程。

ISO 还将大数据处理标准纳入人工智能标准体系，包括 ISO 20546（大数据概述和词汇）和 ISO 25047（大数据处理参考架构）。基于现有的大数据标准，ISO 还在制定 ISO 5259（统计分析和机器学习的数据质量）、ISO 24668（大数据分析过程管理框架）和 ISO 8183（数据生命周期框架），这些标准将作为人工智能数据处理系统的要求。

在人工智能算法的技术要求方面，ISO 的 WG5 工作组发布了 ISO 24372，该标准对现有的人工智能算法进行了分类。该标准描述了人工智能系统和计算方法的计算特征，将其分为知识驱动方法（如专家系统）和数据驱动方法（如监督学习、非监督学习和半监督学习）。该标准详细列出了具体计算方法（如知识图谱、决策树、生成对抗网络等）的技术要点、主要计算特征和应用场景。

在人工智能系统标准方面，中国电子工业标准化技术协会（China Electronics Standardization Association，CESA）提出了针对人工智能系统框架的团体标准，将人工智能系统分为 8 个部分，并为每个部分规定了基础功能要求，例如数据标注支持、算法统一注册和管理等。例如，CESA 1040 标准对机器学习的数据标注流程、标注方式和输出形式提出了要求；CESA 1034 标准对不同场景下小样本机器学习算法的训练数据类型和数据量进行了规定；CESA 1197、CESA 1198、CESA 1199 标准分别对图

像合成、视频图像审核、字符识别算法提出了功能和性能要求；CESA 1035 标准规定了音视频和图像分析算法接口的格式；国标 GB/T 40691-2021 则规定了情感数据计算中的功能性要求，包括情感表示、识别、决策和表达。

1.3.3 智能运维的现有标准

国际电信联盟（ITU）为 5G 网络架构（IMT-2020）建立了 SG13 标准组，其中 Y.3170 系列标准专注于人工智能技术在未来网络运维中的应用。Y.3172 提出了机器学习的总体框架，类似于 ISO 23053 的机器学习流水线处理过程；Y.3174、Y.3176 和 Y.3179 对数据处理系统、应用市场和机器学习服务化提出了详细要求；Y.3170、Y.3175、Y.3177、Y.3178 和 Y.3180 则针对网络运维服务的特定场景提出了功能性和技术要求。Y.3173 根据业务需求、数据收集、分析、决策和机器行为映射，定义了从人工运维到完全无人运维的 5 个智能管理等级。此外，ITU 的通信维护标准 M.3080 提出了 AITOM（Artificial Intelligence enhanced Telecom Operation and Management，人工智能增强的电信运营与管理）框架，该框架是在原有 SOMM 框架的基础上，结合 Y.3172 的机器学习技术形成的总体技术架构。

类似地，ETSI 针对网络运维场景建立了智能网络工作组 GS ISG ENI，并提出了一系列智能运维标准。ETSI GS ENI 005 定义了整体运维系统框架，包括数据获取、知识管理和模型构建等模块的具体功能要求；ETSI GR ENI 001 列举了 20 多个网络智能运维场景，并对每个场景进行了用例分析，明确了参与角色和执行流程。此外，ETSI GS ZSM-001 标准也涵盖如何利用人工智能辅助运维，主要关注系统运维数据的收集和处理要求。

在国内，中国电子节能技术协会和 CAICT 也推出了相关团体标准。中国电子节能技术协会针对数据中心的智能运维场景提出了具体功能性要求；CAICT 发布的团体标准 T/CCSA 382.1-2022 定义了智能运维场景的成熟度等级及功能要求。

国家标准 GB/T 43208.1-2023《信息技术服务 智能运维 第 1 部分：通用要求》于 2023 年 9 月发布，2024 年 4 月实施。GB/T 43208.1-2023 确立了智能运维框架，规定了智能运维组织的组织治理、智能运维场景实现和能力域的通用要求，针对数据、算法、技术 3 个智能运维能力的关键要素从治理层面提出要求。

国家标准 GB/T 43208 由 4 个部分构成，包括通用要求、运维数据治理、运维算法治理和运维技术治理，各部分之间的关系如图 1-1 所示。

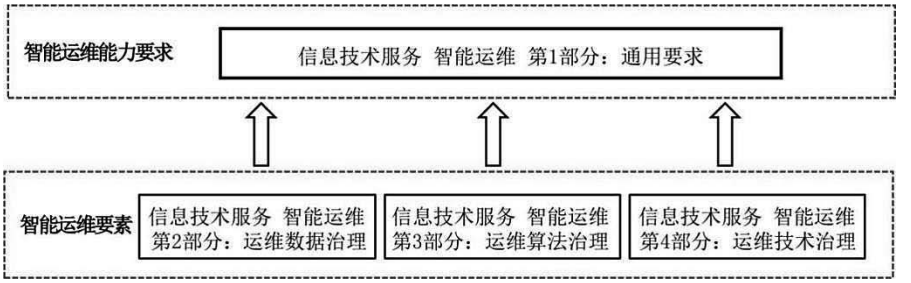

图 1-1　GB/T 43208 各部分之间的关系

第 1 部分：通用要求。目的是为智能运维组织提供智能运维框架，指导组织从组织治理、智能运维场景实现和能力域 3 个方面开展智能运维建设，持续提升智能运维水平，实现运维目标。

第 2 部分：运维数据治理。目的是为智能运维组织提供运维数据治理框架，指导组织对能力域中的数据要素进行治理，为智能运维建设提供高质量的运维数据，有效地支撑智能运维场景的实现。

第 3 部分：运维算法治理。目的是为智能运维组织提供运维算法治理框架，指导组织对能力域中的算法要素进行治理，为智能运维建设提供安全、可靠、有效的运维算法，挖掘运维数据的价值，赋能运维场景的实现。

第 4 部分：运维技术治理。目的是为智能运维组织提供运维技术治理框架，指导组织对能力域中的技术要素进行治理，为智能运维建设提供技术应用的原则、方法和要求，支撑智能运维场景的实现。

第 2 章

智能运维框架

本章主要介绍国家标准 GB/T 43208 提出的智能运维总体框架，该框架从组织、场景和能力 3 个维度列出了智能运维建设中的关键要点，旨在为企业的智能运维能力建设提供明确的指导。

2.1 整体框架

国家标准 GB/T 43208 提出了智能运维框架，由组织治理、场景实现、能力域 3 部分构成。组织治理涵盖组织策略、管理方针、组织架构、组织文化以及相关方需求和期望。场景实现包括场景分析、场景构建、场景交付和效果评估 4 个过程。能力域包括数据管理、分析决策、自动控制等能力域，每个能力域由若干能力项构成，而每个能力项又由 7 个要素组成，这些要素是人员、技术、过程、数据、算法、资源和知识。

场景实现是智能运维能力构建的核心，既是需求起点，也是效果体现。实现智能运维场景需要构建数据、算法和自动化能力，这些能力通过 4 个关键过程不断迭代提升。组织治理则驱动智能运维能力的持续构建，确保企业能不断提升和实现智能运维场景。

智能运维的智能特征包括：能感知、会描述、自学习、会诊断、可决策、自执行、自适应。智能运维框架如图 2-1 所示。

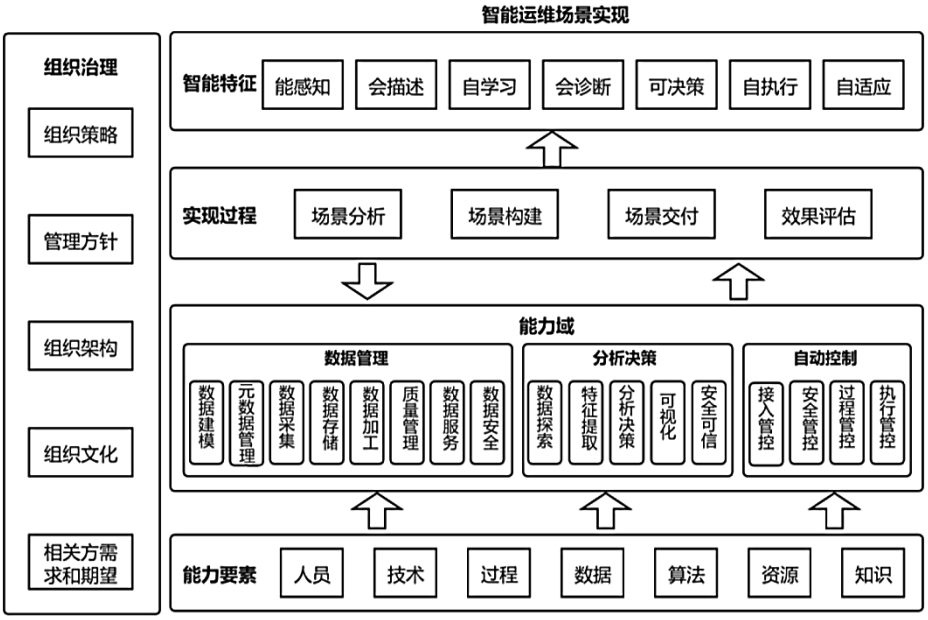

图 2-1　智能运维框架

2.2　组织治理

在智能运维建设过程中，各类场景和需求会不断涌现。如果仍然依赖各自为政的开发方式，而不对不同场景的数据和技术进行整合与共享，就会导致重复建设，并增加后续迭代的复杂性，最终导致前台系统繁杂而后台支撑不足。因此，企业在构建智能运维能力时，需要从组织层面进行统一规划和资源整合。

通过组织策略、管理方针、组织架构、组织文化及相关方需求和期望对其组织进行完善，以指导组织开展智能运维能力的建设和智能运维场景的实现。组织应建立提升智能运维能力的策略，在管理原则的指导下建立智能运维方针，建立符合智能运维管理要求的组织架构，符合智能运维持续发展的组织文化，明确智能运维不断变化的组织环境。

2.3 场景实现

由于运维场景的划分粒度不同，智能运维的场景数量非常庞大。例如，多个场景可以组合成混合场景，混合场景也可以拆分成多个单独场景分阶段实施。因此，应关注通用的智能运维场景实现，而非针对特定场景类型。

智能运维场景的实现是一个需要持续优化的过程，旨在围绕质量可靠、安全可控、效率提升和成本降低的运维目标，不断迭代调优来提升运维智能化水平。我们通过 4 个关键过程构建智能运维场景：

（1）场景分析：通过前期的调研和评估，确定场景构建的方案和计划。

（2）场景构建：根据既定方案和计划，进行场景相关能力的建设。

（3）场景交付：在场景构建完成后，实施交付及相关配套活动。

（4）效果评估：在场景交付后，检查是否达到了预期效果，并为下一阶段的迭代设定目标。

表 2-1 列出了部分常见的运维场景。

表2-1 常见的运维场景

场景名称	场景描述	关键指标	智能特征	目　　标
告警聚合	该场景通过算法或规则，将无效和重复等相同原因触发的告警合并为一个告警	告警聚合率=1－聚合后告警数/总告警数	会诊断	质量可靠：在事前、事中、事后的各方面，有效提高运维服务对象的运行稳定性和可靠性
异常发现	该场景通过实时收集运维对象的业务交易量、成功率、耗时、系统性能、日志等数据，利用机器学习训练历史数据运行模型，实时检测运行数据，实现快速发现运维对象的运行异常状态	异常发现准确率=有效告警数/总告警数； 异常发现漏报率=（应告警数－有效告警数）/应告警数	自适应、自学习、能感知、会诊断	
故障影响分析	该场景通过综合分析业务、应用系统间的依赖关系和配置数据，实现快速准确地推断某个故障的影响范围和程度	故障影响分析准确率=影响范围分析正确的故障数量/故障总数	可决策、会描述	

（续表）

场景名称	场景描述	关键指标	智能特征	目　　标
故障根因定位	该场景通过排障决策树、对象关联图谱、故障传播影响分析等方式，实现对版本变更、业务参数调整、代码逻辑或基础设施故障带来的各种大规模、并发异常告警进行根因分析定位和根因故障推荐	故障根因定位准确率=准确推荐根因故障数/总推荐根因故障数；故障根因定位覆盖率=准确推荐根因故障数/总故障数	能感知、可决策、会诊断、自学习、自适应、会描述	质量可靠：在事前、事中、事后的各方面，有效提高运维服务对象的运行稳定性和可靠性
故障预测	该场景通过收集和处理运维对象历史运行数据和故障数据，建立不同技术领域的故障模型，提取故障特征，归纳故障演化规律，实现对运维对象运行趋势的动态预测	故障预测准确率=准确预测数/总预测数	自学习、会诊断	

2.4　能力域

国家标准 GB/T 43208 将智能运维的能力建设划分为 3 个主要方面：数据管理能力、分析决策能力和自动控制能力。在构建智能运维场景时，需全面评估和改进这些方面，以确保在实际应用中能够基于高质量的运维数据，利用算法进行合理判断，并根据需要自动化地执行运维操作。

1. 数据管理能力领域

数据管理能力领域涵盖对运维数据进行全面的生命周期管理和应用的各项能力，包括确保数据的高质量、全面覆盖、互联融合，并满足时效性需求。该领域包含以下 8 项能力：数据建模、元数据管理、数据采集、数据加工、数据存储、质量管理、数据服务和数据安全。

2. 分析决策能力领域

分析决策能力领域涉及使模型能够自主预测、判断和行动的能力。它通过筛选、整合和处理相关运维数据，结合规则和算法模型，为智能运维场景提供决策支持。该

领域包括 5 项核心能力：数据探索、特征提炼、分析决策、可视化和安全可信。

3. 自动控制能力领域

自动化能力是显著提高运维效率的关键因素。它不仅能替代人工操作，通过与各种工具、平台和流程的有效配合来执行大量重复性的日常运维任务，还能推动运维操作的标准化，增强流程的可控性。结合数据和算法形成的决策能力，进一步推动运维向无人化的方向发展。自动控制能力领域旨在通过设备、软件和服务提升运维活动的自动化水平，实现目标预期的自动执行，从而提高运维效率并减少人工干预。该领域包括 4 项关键能力：接入管控、安全管控、过程管控和执行管控。

下面的示例 1 和示例 2 展示了如何在具体运维场景中对能力项进行详细解析。能力域是由一系列智能运维能力组合而成的。每个子能力域中的具体能力项围绕 7 个能力要素提出了一系列要求，运维人员可以根据这些标准作为参考，按步骤实施智能运维场景，或依据标准内容优化已有的智能运维场景。

示例 1：场景能力解析

（1）场景：智能日志异常诊断。

自动收集各类型的日志，自动提取各日志模板，建立所有日志模板运行基线，自动发现基线异常并进行告警，在提高故障发现率的同时，无须大量人工干预。

（2）目标：效率提升，成本降低。

（3）活动：分析。

（4）智能特征：自学习、会诊断。

（5）能力域：分析决策能力域。

（6）能力项：特征提炼。

（7）能力要素：包括人员、技术、过程、数据、算法、资源及知识。

① 人员

- 运维场景研发团队安排具备特征工程等相关背景知识和研发能力的成员制定日志模板提取方案，至少应包含日志解析、特征颗粒度定义和特征抽取方案。
- 运维场景研发团队协调日志产生方对日志模板识别结果进行评估。

② 技术

- 针对不同类型的日志数据，采用不同的特征提取方式。为了便于特征提取自

由格式的非结构化日志需先进行规则解析，而 JSON 等结构化日志则可直接进行特征提取。

- 针对日志模板提取场景，利用 NLP（Natural Language Processing，自然语言处理）等技术将无结构化日志转化成结构化数据。

③ 过程

- 实时解析已收集的日志明细数据，根据解析后不同的日志类型自动选择不同算法，产生多个日志模板。
- 系统持续跟踪日志的变化情况，自动增加或删除日志模板，并按需协调日志产生者、该运维场景使用者等关联方对日志模板分析结果进行识别、判断和反馈，实现日志模板的生命周期管理。

④ 数据

- 快速获取各种日志模板的原始数据，如日志类别、模板关键词、模板生成速度、模板数量等。
- 记录已生成的各明细日志模板，包括模板特征、日志内参数的变量分布等。

⑤ 算法

- 针对日志类型的运维数据，使用日志模板提取 FT-Tree、DBScan、符号分隔、关键字匹配等算法进行结构化转换。
- 针对日志中参数的指标类型运维数据，使用小波分析等算法进行周期特征提取，使用 ARIMA、线性回归等算法进行趋势特征提取，包括统计特征、拟合特征和分类特征等。

⑥ 资源

- 根据日志的规模和分析日志的实时性要求，配置适当的 Flink、Spark 等大数据计算集群。

⑦ 知识

- 结合专家经验和自动提取的日志模板现状，对重要或者高频使用的日志建立日志标准规范，包括格式要求、变量分布取值范围要求等。
- 具备特征提炼中的规则，形成可对特征提炼有效性进行识别、判断、优化和补偿的方法。

示例 2：场景能力解析

（1）场景：智能日志异常诊断。

自动收集各类型的日志，自动提取各日志模板，建立所有日志模板运行基线，自动发现基线异常并进行告警，在提高故障发现率的同时，无须大量人工干预。

（2）目标：效率提升，成本降低。

（3）智能特征：能感知、自学习、会诊断、可决策、自执行。

（4）活动：分析。

（5）能力域：分析决策能力域。

（6）能力项：分析决策。

（7）能力要素：包括人员、技术、过程、数据、算法、资源及知识。

① 人员

运维场景研发团队安排具备异常检测算法能力的成员承担日志模板异常检测模型的设计与研发、实现规则和应用等工作。

② 技术

- 采用大规模日志分类模型训练框架技术。
- 考虑采用日志多维定位和关联分析技术。

③ 过程

- 为每个日志模板建立运行动态基线（主要包括数量、关键变量分布范围等），并持续实时训练。
- 为每个单位时间段建立日志模板占比的动态基线，并持续实时训练。
- 实时检测单个日志模板和单位时间段内日志模板占比是否偏离动态基线。

④ 数据

- 形成动态基线数据。
- 建立异常检测指标，包括漏报率（异常被当作正常的个数/异常的个数）、误报率（正常被当作异常的个数/正常的个数）等。

⑤ 算法

- 通过统计模板出现的频次变化并使用时序异常检测进行检测。

- 通过长短期记忆（Long Short-Term Memory，LSTM）算法对模板出现的顺序规律进行检测。
- 通过词汇信息单词嵌入、语义单词嵌入等自然语言处理技术对模板的语义进行分析检测，实现对运维日志型数据的规律挖掘和异常发现。

⑥ 资源

- 根据日志的规模和分析日志的实时性要求，配置适当的 Flink、Spark 等大数据计算集群。

⑦ 知识

- 告警策略：总结归纳不同日志类型的有效告警策略，包括基线敏感度、异常频次告警规则、稀有日志告警策略等。
- 算法应用指南：为不同日志类型和场景标识有效的日志异常检测算法。
- 场景应用指南：总结归纳不同日志能力边界场景，以及不适用的场景。