爱立信白皮书
BCSS-25:024439
2025年10月

ERICSSON

# 白皮书 – AI智能体在电信网络架构中的应用

# 目录

# 引言

自智网络之旅早已启动，但直至近期才开始显著加速。AI智能体、生成式AI（GenAI）及大语言模型（LLM）凭借强大的自主能力，预计将成为提升网络效率、改进客户服务与运营管理的关键组件。

本白皮书将明确AI智能体的定义，并以TM Forum（TMF，电信管理论坛）制定的意图管理架构为主要案例，展示其在移动网络架构中的应用实践。我们还探讨了其他潜在应用场景，例如助力移动网络优化签约用户与企业所用智能体之间的通信。

我们将深入探讨前期白皮书提出的概念与分析框架，包括《定义AI原生：高级智能电信网络的关键赋能技术》[1]、《意图驱动网络：实现自智网络的关键步骤》[5]以及《5G网络生命周期管理的认知推理》[2]。

# AI智能体:定义与分类体系

针对业界对AI智能体在网络中角色与任务的多元解读,我们需明确智能体与AI智能体的本质内涵。

**智能体**

智能体是被授权代表个人或实体独立采取行动、制定决策并自主发起任务的自主系统。

智能体以目标为指引,通过传感器、协议、数据流或其他智能体交互等机制感知环境,并运用规则、编程逻辑或学习模型处理信息,最终生成输出、执行行动、使用工具甚至运行代码以实现目标。

智能体可在运行时与环境交互,可随时间存储与检索信息,既可独立运行,也能通过智能体间通信实现协同。其计算表达能力覆盖从确定性规则行为到图灵完备推理(Turing-complete reasoning)的完整谱系,从而实现不同层级的适应性、决策与规划能力。

**AI智能体**

AI智能体是智能体的一个子类,运用机器学习技术持续更新其内部知识(有时称为记忆),从而动态适应不断变化的条件。

AI智能体形成一个从受限制(受人为设定约束)到无限制(具备内部逻辑与目标修改能力)的连续谱系。尽管存在编排器(Orchestrator)、协调器(Coordinator)和执行器(Executor)等多种角色与组织模式,本分类体系着重从AI/非AI、受限/无限制维度进行界定。

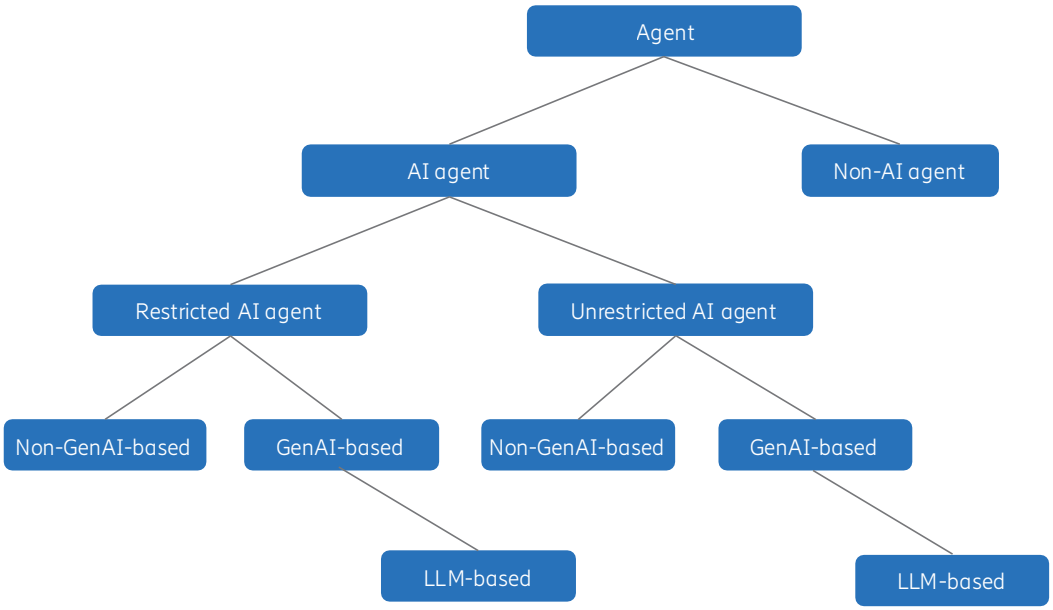



图1:AI智能体分类体系

通过这种方式,我们即可界定受限智能体与无限制智能体之间的边界,从而确定是否及在何种情况下允许不同类型的智能体存在,并反映在架构中。尽管两类智能体存在多种变体,但在下述情况下,受限智能体将转化为无限制智能体:

- **内部逻辑修改:** 覆盖人类编程限制
- **目标体系重构:** 超越人类预设目标边界

此处值得特别说明的是,基于生成式AI的智能体包含一个特定子类——Copilot。这是一种基于大语言模型(LLM)的受限智能体,作为人机交互接口(HMI)与人类协同工作。Copilot通过利用大语言模型(LLM)的自然语言深度理解能力来改善人类绩效。

# AI演进之旅与网络转型

在5G及未来6G技术的推动下，现代电信网络持续演进，导致网络复杂性不断增加，对运营自动化的需求日益迫切。若缺乏自动化，传统网络运营成本或将难以为继，迫使厂商与运营商（CSP）应对此类挑战。自动化既能满足这一需求，又赋能网络更灵活快速地适应客户需求的变化。

通过利用正确的数据并发挥我们在最关键网络领域的深厚专长，AI可有效驱动自动化进程。在此基础上将AI嵌入产品组合，能在运营效率、客户体验、业务增长与可持续发展等多维度创造最大价值。

在6G时代，AI与网络的协同效应将更为关键——AI将作为关键原生组件，塑造网络架构、能力与服务，实现最小化人力干预的意图管理，最终达成零接触运营。

与此同时，生成式AI与AI智能体等新兴技术的出现进一步增强了这些能力，并在多个领域展现出应用潜力，包括：

- **网络运营效率提升：**生成式AI可实现动态网络策略与配置，持续监控网络流量，检测异常状态，并自动响应潜在威胁或效能瓶颈，从而降低运营成本并减少对人工干预的依赖。

- **预测能力构建：**AI智能体可以分析海量网络数据，精准预测拥塞或硬件故障等潜在问题，并主动启动应对机制以增强网络可靠性，延长运行时间。
- **实时决策优化：**生成式AI能基于带宽需求与时延要求等因素生成最优路由路径与资源分配策略，在运行时动态实施这些策略并持续适应网络条件变化。
- **弹性扩展与适应能力：**AI智能体可动态响应持续变化的运营需求与条件，实现对大规模网络的高效管理。

尽管优势显著，在网络中部署AI智能体仍面临诸多挑战：包括与现有基础设施集成、管理并保护海量数据安全的同时确保隐私，以及防御网络攻击。此外，保障系统稳健性与可信性需要对智能体行为进行严格评估、观测与持续监测。

上述并未穷尽的潜力与挑战清单，足以说明智能体系统可能具有的高度复杂性。我们将在后文深入分析部分挑战，其他挑战则仅为保持完整性而简要提及。

# AI智能体与网络架构

运营商（CSP）正步入转型阶段，借助现代AI技术，推动网络运营升级与复杂任务全自动化，使AI及AI智能体技术能在移动网络中部署。当前的5G移动网络已准备就绪并具备承载终端用户AI智能体流量的能力，而向6G的演进将为运营商创造更多机遇——既可在移动网络中应用AI智能体，也能开放面向应用领域AI智能体的服务。

基于AI智能体的定义，它们将如何体现在TM Forum（TMF）、3GPP及开放无线接入网（O-RAN）联盟等标准组织制定的功能架构中？要回答这个问题，需先分析AI智能体的潜在应用场景，并评估其对功能架构的影响及具体影响方式。

作为一种通用实现技术，AI智能体可用于多种目的。为更具体化，下文提供若干示例，展示AI智能体在不同网络域的应用及其对功能架构的潜在影响。

AI原生架构的一个方面是智能无处不在[1]。从商业与技术维度考量，AI功能可部署于任何网络域、协议栈层或物理站点。从这方面讲，AI智能体是AI功能的一种变体。

智能无处不在意味着数据与必要的计算资源需在所需位置随时可用。这需要通过分布式基础设施有效管理信息——该设施应具备数据类型无关性，同时允许对AI及AI智能体工作负载的适当访问。

网络通过各种使能技术不断完善，实现全自动化管理已成为核心诉求。人类仍将保持控制权，但其角色转变为提出需求而非发出具体操作指令——这一特性被称为“零接触”（Zero-touch）运维。

AI智能体作为技术工具箱的新工具，能以结构化、简化的方式解决自动化难题。因此，我们应聚焦AI智能体能做什么，而非具体实现方式。

**意图管理功能智能体**

当网络实现完全自主运行时，控制环路与决策过程无需人工参与。自智网络可独立完成部署、配置、维护（包括监控、优化与自愈）及退役生命周期管理。向自智网络演进的一个重大步骤是引入基于意图的操作[4][5]——人类交互仅限于通过意图表达网络需满足的需求。根据TMF术语，这对应自智网络级别提升[3]。

TM Forum定义的自智网络架构[7]由多个自治域构成，每个域实现意图管理功能（IMF），并与其他自治域交换意图。每个域均包含闭环控制环路与以知识为核心的域内智能。

意图管理功能可被视为智能体，因其具备自主观测、决策、行动并与其他智能体交互等能力。在这一架构下，意图管理功能可调度并协调多个其他智能体，以满足其自身的意图需求，并基于这些需求实现最优的网络性能。

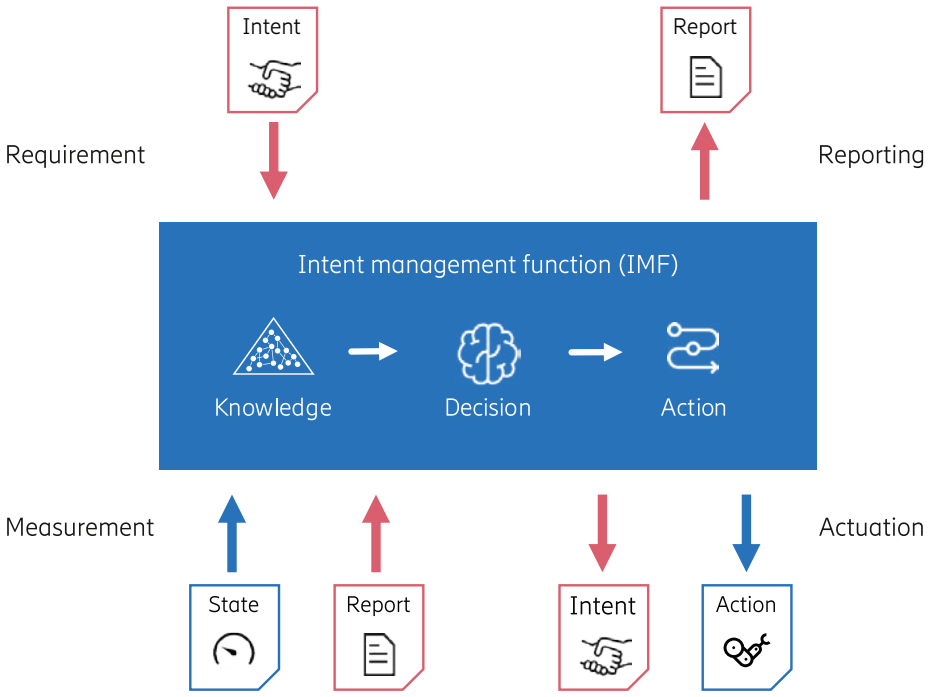
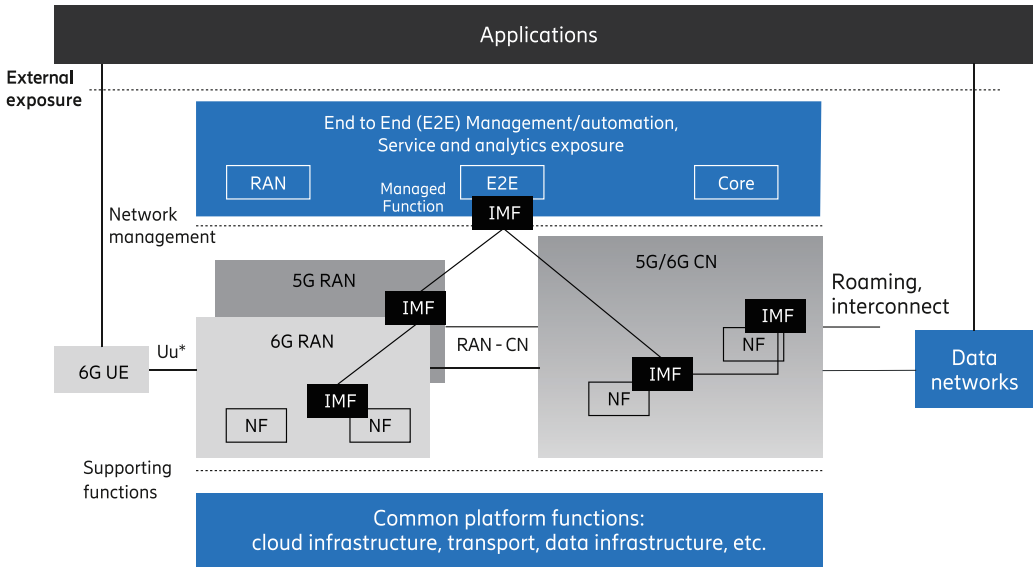



图2：意图管理功能（IMF）详细视图

如图3所示，我们可将意图管理功能映射至网络架构。该映射可进一步细化——相关标准化工作已在推进中，包括意图管理功能间通信接口的标准化[12]、[13]、[14]、[15]。

由于意图管理功能是自主组件，它们非常适合AI智能体实现。若通过AI智能体实现意图管理功能，智能体间通信将遵循TMF定义的功能接口规范。




* 连接通用陆地无线接入网（UTRAN）与用户设备（UE）的无线接口。

图3：拟议6G网络架构中的意图管理功能部署

**流程自动化智能体**

意图可显著简化管理并加速网络中新服务的引入，进一步推动了全自主系统愿景的实现。然而，由于当前仍存在大量依赖人工参与的环节，要实现“零接触”愿景仍需突破多重技术难关。

AI智能体可自动完成传统上由人工主导的流程，例如网络运营商与企业客户之间的服务订购。在现有模式下，企业客户向网络运营商订购服务时，运营商的客户销售代表需要执行冗长的流程，包括查询产品或服务目录、与客户协商、向订单处理系统提交订单等。

当AI智能体扮演Copilot的角色时，可自动执行这些步骤，实现个性化产品推荐、动态定价策略与加速服务交付。

**自动化网络管理智能体**

将AI智能体集成至网络管理层，将在未来网络管理的两大核心领域实现显著的智能驱动改进：运营效率提升与网络配置优化。

**运营效率提升**

AI智能体可自主利用网络指标数据，精准识别遥测数据中可能预示安全威胁或运营异常的异常模式。

为实现更具前瞻性的运维管理，使AI智能体基于历史网络数据执行预测性分析与处置决策，将有效减少潜在故障与性能降级，显著减少停机，降低维护成本，同时确保未来网络具备更优异的可靠性与稳定性。

通过自动获取所有所需上下文信息并进行智能推理，AI智能体将简化未来网络管理运维任务，消除当前网络工程师在不同接口间手动进行上下文切换与分析的繁琐操作。

**网络配置优化**

如前所述，通过嵌入到支持全管理域复杂分析与决策的管理平台中，AI智能体将成为在网络管理层实现意图驱动组网与运营的关键使能技术。

例如，在平台服务或运行于这些平台的应用程序中（如服务管理与编排（SMO）平台中的rApp[11]），智能体间通信可通过O-RAN支持的rApp间通信方法实现。

另一关键贡献体现在网络规划与切片编排领域。通过分析使用趋势并预测未来需求，电信运营工程师与业务合作伙伴将能更有效地分配资源，并规划必要的基础设施升级或扩容。

这方面的一个例子是动态网络切片，即将网络分区为针对特定应用或用户需求的虚拟切片。AI智能体将在运行时管理这些切片，确保多样化用例获得最优性能。

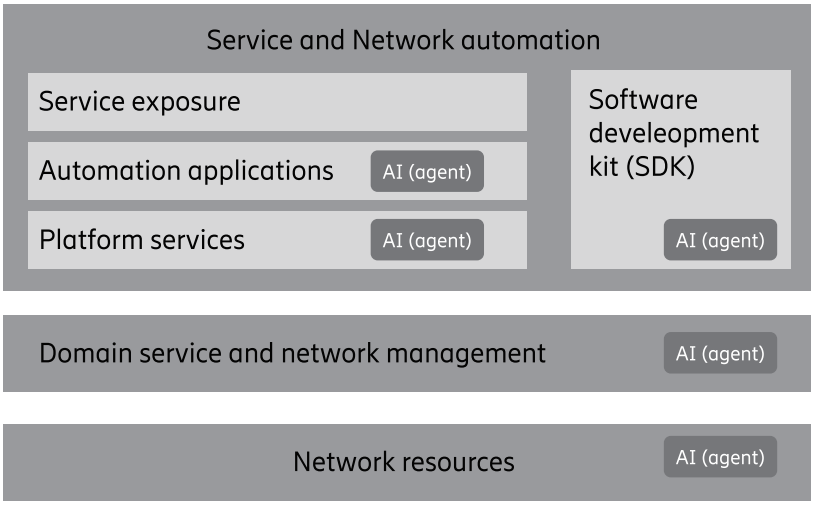



图4：支持高级服务与运营智能的网络管理层AI智能体

### 3GPP核心网智能体

若在网络功能内使用AI智能体作为实现技术，则3GPP核心网架构几乎无需改动[8]。

例如，AI智能体可在策略控制功能（PCF）中发挥积极作用。默认情况下，当运营商设置（声明式）策略时，策略控制功能被授权自主制定策略决策。采用AI智能体方案后，策略控制功能即成为代表运营商的智能体。

其他网络功能也可采用类似方案。若两个不同网络功能中的智能体需要通信，可通过服务化接口（SBI）通信的功能扩展来实现。

尽管可采用AI智能体实现功能，我们仍需综合评估其效率与方案改进价值。鉴于本白皮书旨在揭示此类技术的潜力并厘清所有影响维度，具体实施方案需在后续研究中进行均衡评估。

### 应用域智能体的网络支持

现有网络承载用户间通信流量，有时也支持其AI智能体间的交互。运营商可通过开放网络服务（如定位、差异化连接与网络切片）为这些用户应用提供额外的支持。

当前，网络服务开放应用编程接口（API）呈现多层结构：既有网络开放层接口，也有应用域层接口（采用CAMARA与GSMA Open Gateway倡议的API标准）。

此类API可为AI智能体特定功能提供额外的支持，如智能体注册与发现、认证及授权。同时，需通过适当的授权机制保障网络稳健性与完整性，并建立规范，明确智能体可共享的信息范围与可讨论的议题领域。

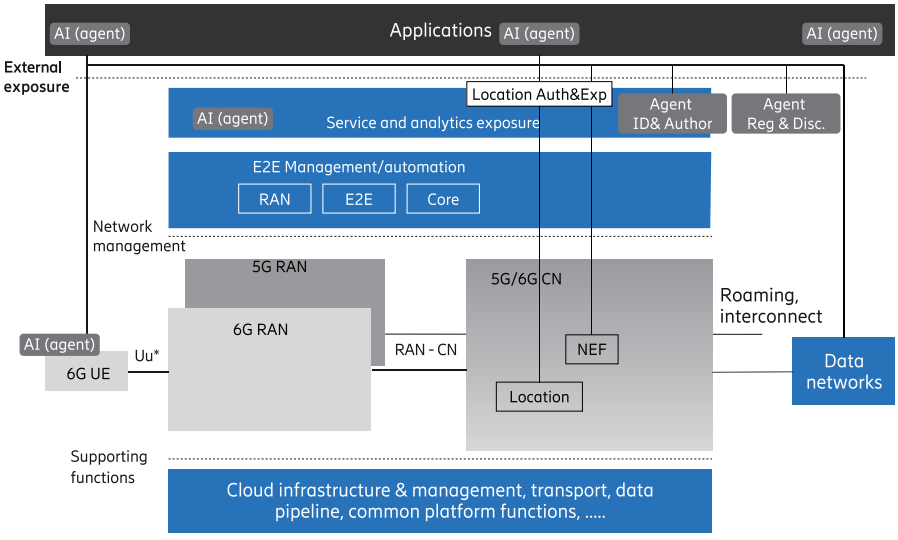



图5：应用域智能体的网络支持

# 模型上下文协议（MCP）

模型上下文协议（MCP）[9]已在AI领域迅速获得广泛普及，该协议建立标准的客户端-服务器架构，通过统一接口向基于大语言模型（LLM）的智能体开放工具、资源与提示，从而访问各类服务。

为明确MCP在电信领域的潜在定位，我们需认识到将现有的独立API调用封装为MCP服务器工具并非最优方案，因为API与MCP服务器不能直接互换。API专为开发者设计，用于执行精确的底层操作，参数严格；而智能体则通常执行高级任务与行动，通过自主推理与意图驱动交互实现特定目标。

MCP服务器通过在传统API之上增加一个对话式或智能体友好层来利用底层API。MCP工具的作用是将多个底层API调用抽象为连贯的高级工具，代表智能体为实现特定目标可调用的任务或能力。

基于此认知，图6展示了MCP在电信领域的一个潜在应用场景。在此场景下，运营商为开放给应用层的网络服务提供MCP服务器。这与前文所述的网络服务开放模式相似——通过API为AI智能体特定功能提供增强支持。Vonage推出的Telephony MCP服务器[16]便是该角色的一个早期实践范例。

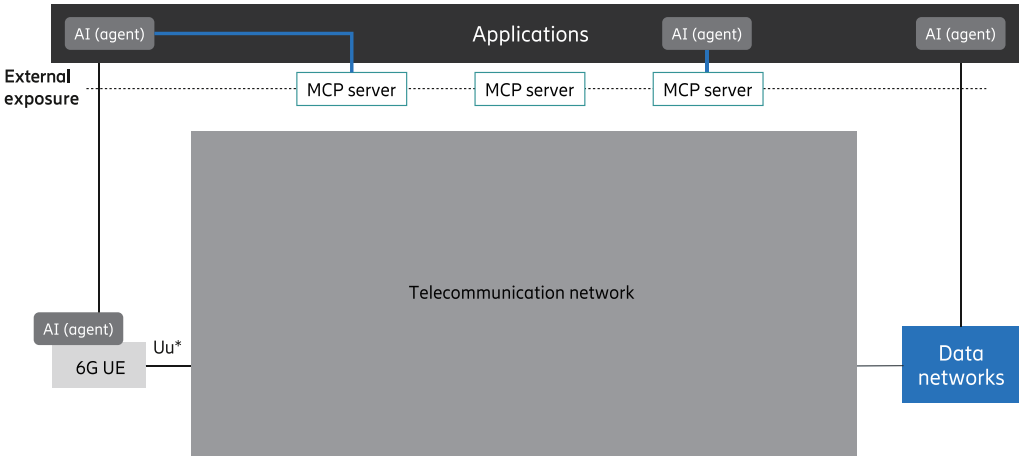



图6：电信网络架构中的MCP服务器部署

MCP的另一潜在角色是单纯作为使用AI智能体构建内部网络服务的实现技术。

# 智能体间通信

智能体间（A2A）通信协议[17]是模型无关的通信标准，旨在实现AI智能体间交互，促进最小人力干预下的可扩展协作。A2A协议标准化了智能体间交换消息的结构，包括目标、能力、状态更新、请求与承诺等。作为MCP的补充，A2A旨在实现涌现式（emergent）、自组织且可扩展的AI智能体生态系统。

由于AI智能体属于具体实现技术，当用于实现现有标准化网络功能时，智能体应使用现有功能接口而非通用智能体接口（如A2A）。例如，若采用AI智能体实现部分意图管理功能，则应通过TMF意图管理框架及协议进行意图传递。

其设计动机源于“关注点分离”（separation of concerns）原则，即一个领域的实现技术应独立于另一领域的实现技术。换言之，两个通信功能实体不应假设对方基于智能体架构并使用特定智能体接口。

对于专有接口，应允许智能体根据各智能体的目标灵活选择最优协议（例如A2A）。

# AI智能体系统的稳健性与可信性

在基于大语言模型（LLM）的AI智能体系统中实现稳健性与可信性面临重大挑战——鉴于电信基础设施在这方面的严苛要求及电信API的复杂设计，该问题需给予特别重视。

传统方案采用所谓的“防护栏”（guardrails）技术，包括人类反馈、提示词验证器、输出过滤、审核模型（moderator models）及微调等，使模型符合人类偏好并提升安全性。架构级防护栏（包括工具约束、代码沙箱、思维链监督与检索增强生成（RAG））则可进一步降低幻觉等风险。语法约束解码等其他方法将大语言模型（LLM）的输出限制在形式语法范围内，从而确保句法正确性。然而，这些技术仍无法保证正确性与对齐性。

因此，实现稳健可信的AI智能体需要特别关注以下环节：
- **评估：**在开发与运营阶段分析AI智能体的推理过程、正确性、安全性及任务完成情况。
- **可观测性与监测：**持续监测智能体行为与内部事件，随时间推移优化智能体性能。

AI智能体的评估较传统AI模型更为复杂，因为需要同时考量结果与轨迹。由于需要追踪获得特定结果的所有步骤，使得评估、监控与观测更趋复杂。

# 总结

总之，AI智能体与智能体架构将在电信网络中得到广泛应用。然而，我们应将AI与智能体视为网络架构中各种功能（如意图管理功能、rApp或3GPP网络功能）的实现技术，而非独立功能或独立架构。

智能体架构与智能体的使用绝不能危及网络运行的稳健性与完整性。标准化功能网络架构仍适用于智能体，这为其可观测与可操作范围提供了明确的权限上下文。

这还意味着智能体应驻留在具有清晰接口与授权机制的网络运营域和层级中，同时充分发挥其推理决策能力。

鉴于当前网络架构趋于采用标准化的功能接口方法，AI智能体之间的通信将能够通过现有功能接口实现，例如：3GPP核心网的SBI、rApp间通信（R1接口）以及IMF间通信接口。

AI智能体的实现细节将不纳入标准化范畴，这契合“AI与AI智能体属于实现技术而非架构”的观点。这样，AI智能体就能够灵活使用不同实现方案并以不同节奏演进。

模型上下文协议与A2A等技术为AI智能体领域带来了重要的价值与能力。标准化API将继续支撑大部分网络功能，而模型上下文协议可作为向智能体开放高层工具的抽象层（尤其是在管理与应用领域）。同时，A2A可用作智能体间的内部通信协议，用于在专有实现方案内实现可扩展的智能体间交互。需要强调的是，这两项技术均旨在通过实现更灵活智能的智能体交互来补充API。

下面的两幅总结性图示分别展示了AI智能体在管理与编排域及3GPP功能架构中的潜在部署方案。

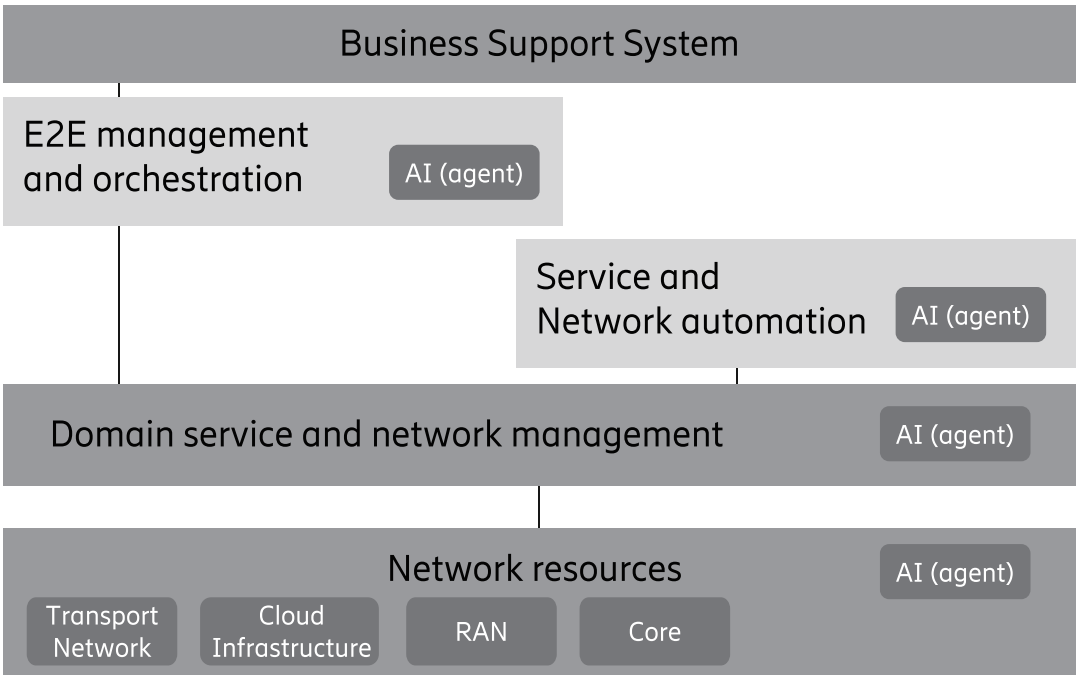



图7：AI智能体在管理与编排域中的潜在应用

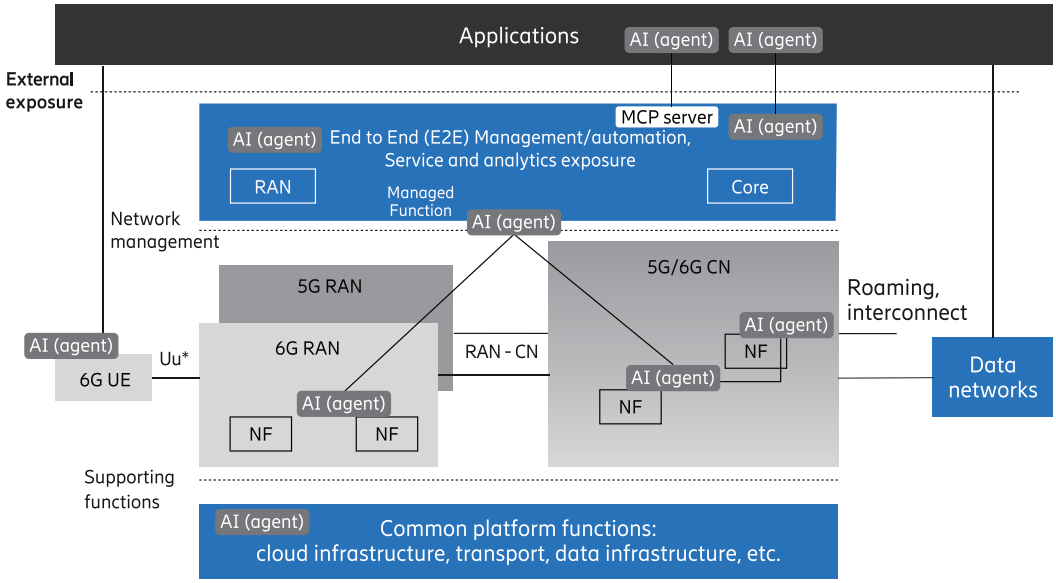



图8：AI智能体在网络架构中的潜在应用

# 结论

AI智能体将在电信领域发挥关键作用，塑造未来网络演进方向。本白皮书重点探讨了它们在5G与6G网络自主运维方面的潜力；明确了AI智能体与电信网络架构的关系；并给出了AI智能体的精确定义，同时强调了稳健性、适应性及运营效率等关键考量。我们建议电信行业领导者确立AI智能体解决方案的长期愿景，将其作为应对当前挑战与把握长期机遇的灵活、可扩展的技术路径。

# 参考文献

1. 爱立信-《定义AI原生：高级智能电信网络的关键使能技术》
2. 爱立信 -《5G网络生命周期管理的认知推理》
3. TM Forum（TMF） -《自智网络等级评估方法（IG1252）》
4. 爱立信 -《基于多层意图运营的自智网络》
5. 爱立信 -《意图驱动网络：实现自智网络的关键步骤》
6. 爱立信 -《如何利用生成式AI提升网络洞察价值》
7. TMF -《自智网络技术架构（IG1230）》
8. 3GPP -《TS 23.501：5G系统（5GS）架构》
9. Anthropic -《模型上下文协议（MCP）》
10. Google -《智能体间（A2A）通信协议》
11. 爱立信 -《SMO赋能智能RAN运营》
12. TMF -《自智网络中的意图管理v1.3.0（IG1253）》
13. TMF -《TMF921意图管理API用户指南》
14. 3GPP TS 28.312 -《移动网络意图驱动管理服务》
15. O-RAN WG1.TR.SMO-INT-R004 -《SMO意图驱动管理》
16. Vonage -《Telephony MCP服务器》
17. A2A

# 作者

**Massimo Iovene**是核心网工程AI专家，拥有超过25年的电信架构、产品实施与客户合作经验。过去几年，他致力于云技术、自动化、运维（O&M）、总拥有成本（TCO）优化及云原生演进等产品战略和演进研究，深入分析市场趋势、行业现状与科研动态。近年来，他主要致力于AI领域及其相关方法的研究，首要目标是将这些技术应用于电信领域，实现网络节点与服务的自动化。

**Leif Jonsson**博士于1998年获乌普萨拉大学（Uppsala University）计算机科学硕士学位，同年加入爱立信研发部门。2018年，他通过与爱立信合作的研究项目，获得林雪平大学（Linköping University）机器学习与人工智能方向的计算机科学博士学位。其研究专注于运用机器学习提升大规模软件开发效能，特别是在传统上难以自动化的复杂任务领域。作为爱立信AI与机器学习专家，他主导AI战略制定，开展机器学习领域指导与教学工作，并推动全公司范围内的机器学习应用研究。

**Dinand Roeland**是爱立信研究院首席研究员，于2000年加入公司。他当前的研究重点是将人工智能技术引入端到端网络架构，以实现自主认知网络。他曾担任多种技术领导职务，包括产品开发、概念开发、原型设计、标准化、系统管理与项目管理。Roeland持有荷兰格罗宁根大学（University of Groningen）计算机架构与智能系统硕士学位（优等）。

**Göran Hall**是CTO办公室网络架构演进（AI/ML）专家。他于1991年加入爱立信，主要从事分组核心网架构领域的开发与标准化工作，曾参与GPRS、WCDMA、PDC、EPC及5G核心网的标准制定与产品研发。2021年加入CTO办公室，负责爱立信产品AI架构原则。Hall持有瑞典哥德堡查尔姆斯理工大学（Chalmers University of Technology）电气工程硕士学位。

**Jörg Niemöller**是分析与客户体验专家。自1998年，他曾在爱立信研究、核心网系统管理与数字服务部门任职，致力于开发智能系统概念与解决方案，推动自主运营并实现零接触愿景。目前，他专注于通过演进产品与标准化将这些技术引入行业。Jörg是TM Forum意图管理指南与模型相关资料的主要作者。

**Paddy Farrell**是数据科学与网络智能专家，专注于将AI技术应用于爱立信网络管理解决方案。2000年加入爱立信以来，他通过运用机器学习、预测分析与自动化技术，在提升网络效率、可靠性与可扩展性方面发挥了关键作用。
Paddy持有电子与软件工程双学位及人工智能硕士学位，致力于推动研究与创新，与客户紧密合作，设计和实施变革网络性能与运营的尖端解决方案。

**Ulf Mattsson**是分组核心网专家，拥有覆盖四代移动通信系统的25年电信行业经验，涉及网络与移动终端开发、架构定义及标准化工作。近年来，他专注于AI/ML架构研究。Ulf持有哥德堡查尔姆斯理工大学（Chalmers University of Technology）硕士学位。