HCLTech | Supercharging Progress™

HCL Tech contribution to AI adoption acceleration



Domenico Convertino

Senior Vice President
HCL Tech

Revenue Intelligence User Forum – 2026

Classification: Internal

Everybody is doing AI

Many telcos have:

GenAI Pilots Copilots Chatbots AI Proof of Concept

Few achieved:

Autonomous Operations
Material cost reduction
Enterprise wide adoption
New, AI driven, revenues

Copyright © 2025 HCLTech | Confidential

What we see globally

AI in telco is becoming an industrial agenda

AI has moved from curiosity to economics	Telecom AI impact is now discussed in terms of revenue, investment and affordability.
Network automation is the front line	The industry is shifting from task automation toward autonomous networks and operations.
AI-native network architecture is arriving	Digital twins, AI-RAN/vRAN and intelligent control loops are moving into operator roadmaps.
Inferencing is redefining infrastructure	Distributed compute, edge inference and sovereign AI are becoming strategic telco themes.
The bottleneck is industrialization	Data quality, integration, governance, workflow redesign and skills decide business impact.

Copyright © 2025 HCLTech | Confidential

HCLTech

AI adoption is not a technology problem

It is an industrialization problem



HCLTech Focus areas for AI adoption

SCALABILITY

- Hybrid cloud fragmentation
- Dependency on individual AI vendors and platforms
- Integration with existing enterprise systems

FINANCIALS

- Bill shock risk
- Cost predictability
- Sustainability



TELCO DOMAIN UNDERSTANDING

- Enterprise knowledge exposure
- Weak domain specialization
- Inconsistent model performance at scale

SECURITY

- Privacy and regulatory exposure
- Security vulnerabilities
- Sovereignty

 Copyright © 2025 HCLTech | Confidential

AI Gateway

01



Gen AI Adoption: main four risks

scaling GenAI usage without a single enforcement point for cost, access, approval and security enforcement

BILL SHOCK

Impact >> Unpredictable spend and unclear project cost allocation.

Shared or directly distributed provider keys prevent granular budget and consumption control.

EXTERNAL KEY USAGE

Impact >> Unauthorized access, credential exposure and policy bypass.

Provider keys may be used from devices, networks or workloads outside the approved HCLTech perimeter.

SECURITY

Impact >> Uncontrolled access and usage of key company assets

Agentics and AI artifacts secure access to company data and legacy applications

FRAGMENTED TOOLING

Impact >> Higher integration cost, vendor dependency and inefficient model selection.

Teams independently integrate different providers and models without coordinated routing or reuse.

It's required a
GOVERNED AI ACCESS LAYER to PROTECT credentials , ENFORCE security, CONTROLS spend and OPTIMIZE model requests

Copyright © 2025 HCLTech | Confidential
HCLTech

Classification: Internal

How CTG AI Gateway makes GenAI Adoption Governed by Design

AI DEMAND REQUESTERS

AI enters through multiple consumption paths

Users
Individual access and experimentation

Applications
Embedded GenAI capabilities

Agents
Autonomous and assisted workflows

GOVERNED CONTROL POINT

CTG AI GATEWAY

One shared control layer between demanded requests and approved AI models or providers

- Identity
- Policy
- Access
- Usage
- Budget
- Audit

Verified before access is granted

ENTERPRISE OUTCOMES

CONTROLLED CONSUMPTION

Predictable spend and attributable project costs

Virtual keys, usage limits and hierarchical budgets control consumption by user, team, provider model

PROTECTED ACCESS

No exposed keys or unmanaged external access

Provider credentials remain inside the Gateway, while identity, source and policy are verified for every request

ENFORCED GOVERNANCE

Consistent accountability and auditable enforcement

Approved users, applications, models and policies are checked before provider access is granted.

ENTERPRISE AI CONSISTENCY

Standardized implementation patterns, reusable capabilities and consistent governance across BUs

The Gateway provides a common consumption layer that enables different teams to use approved models, agents and AI services through the same controls, policies and operational framework, reducing fragmentation and promoting enterprise-wide adoption.

ONE GOVERNED CONSUMPTION LAYER

Secure • Accountable • Cost-controlled • Reusable across ERS

Copyright © 2025 HCLTech | Confidential

HCLTech

From AI Access to an Enterprise AI Operating Model

One common layer to govern AI consumption, protect access and harmonize reusable capabilities across ERS.

CONTROLLED CONSUMPTION
Makes AI consumption attributable, forecastable and manageable across organizational levels.

PROTECTED ACCESS
Credentials and access safeguarded

ENFORCED GOVERNANCE
Controls applied and decisions traceable

ENTERPRISE AI CONSISTENCY
Transform fragmented AI demand into a governed portfolio of approved services



CTG AI GATEWAY

Shared control and consumption layer

IDENTITY & ACCESS
Who and what may connect

POLICY ENFORCEMENT
Which controls apply

USAGE & BUDGET
What is consumed and recorded

AUDIT
Which approved service is used

PILLAR 1

01 FINANCIAL GOVERNANCE & CAPACITY

Attributes usage and cost to users, teams, projects, applications and virtual keys. Applies budgets and warning thresholds. Provide evidence of allocation reviews and budget extensions

PREDICTABLE, ATTRIBUTABLE USAGE

PILLAR 2

02 SECURITY & ACCESS CONTROLS

Identity, credentials, provider access, network policies and audit controls are applied consistently.

CONTROLLED ACCESS BY DESIGN

PILLAR 3

03 POLICY EXECUTION & TRACEABILITY

The Gateway executes approved policies and records decisions. Formal approvals and ownership remain with designated ERS roles.

TRACEABLE, CONSISTENT CONTROL

PILLAR 4

04 AI TOOL HARMONIZATION & REUSE

Approved models, APIs, agents and reusable patterns are made available through a common framework, reducing fragmented tool adoption.

REUSE INSTEAD OF DUPLICATION

ROLE CLARITY

The Gateway applies controls and provides usage evidence.
Business approvals, ownership decisions and formal budget allocation remain with the relevant ERS processes and systems of record.

Copyright © 2025 HCLTech | Confidential

HCLTech

Models

02



GenAI Adoption Challenges: Data Intelligence

From generic models to customer-owned, domain-specialized operational intelligence.

Too Platform Centric

Value can depend on a vendor control plane or OSS stack rather than reusable customer operations knowledge.

Too Generic

General LLMs are not built on purpose for telco.

Too Static

General LLMs improve productivity but do not natively understand telco functional behavior or operational risk.

Too Hard to Own

Customers need a clean boundary between provider IP, customer data, and customer-owned tuning layers.

Copyright © 2025 HCLTech | Confidential

Classification: Internal

AI strategy built on Specialized Language Models

The model builds value in layers with a clear demarcation of ownership and responsibility through identifiable assets

HCLTech Foundation Layer

Includes SLM and RAG built in-house using public knowledge, telecom expertise, IP, runbooks, evaluation, and governance frameworks

HCLTech Specialization Layer

Focuses on tuning functional and behavioural aspects, adapting to environment, vendor stack, cloud, and operating models

Customer Ownership Layer

Customers retain ownership of the final layer, customizing tuning based on their data, policies, and local context

CTG AI Specialized Model



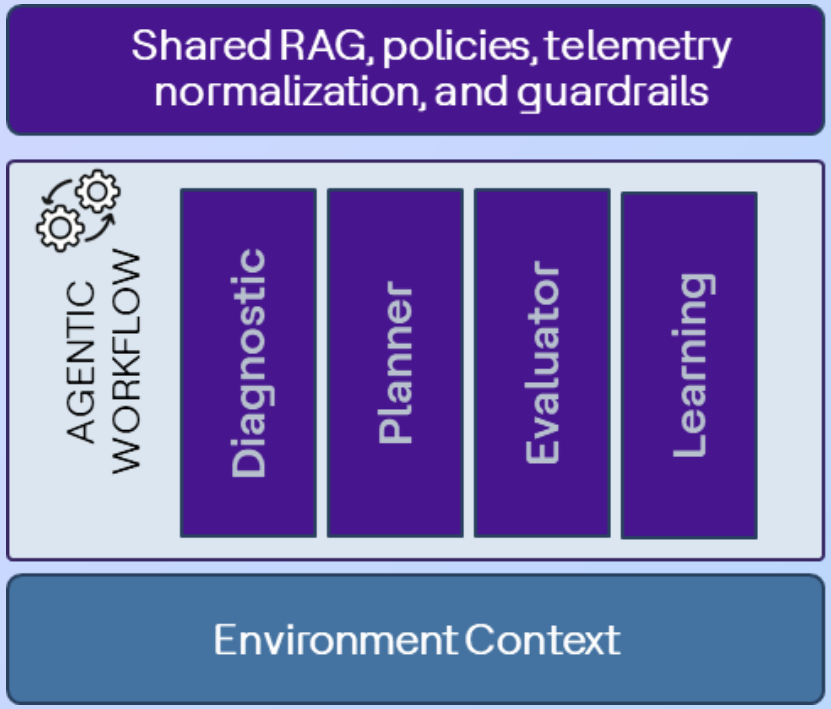
Copyright © 2025 HCLTech | Confidential

Classification: Internal

AI strategy built on Specialized Language Models

Single approach for multiple domains

- Functional SLMs learn repeatable operator behaviors such as diagnose, plan, evaluate and learn.
- Environment layers capture the context that makes telco operations hard: topology, vendor stack, cloud platform, policy, and workflow.
- The result is a governed portfolio of smaller models instead of one opaque model trying to master everything.





Copyright © 2025 HCLTech | Confidential

Agentic

03



GenAI Adoption Challenges: Scaling Agent Ecosystems

Industrial agent adoption requires openness, lifecycle governance, integration and orchestration.

Vendor Lock-In

Avoid dependency on a single agent platform, model provider or proprietary framework that limits future flexibility.

Lifecycle Management

Manage agents from design to deployment, monitoring, versioning, retirement and continuous improvement.

Ecosystem Integration

Connect agents seamlessly with enterprise applications, data sources, APIs, workflows and existing security models.

Agents Orchestration

Coordinate multiple agents, tools and tasks to ensure reliable execution, handoffs and end-to-end process automation.

Copyright © 2025 HCLTech | Confidential

Classification: Internal

ART: Open Agentic Framework

Plug 3rd party agents into ART through open, standard interfaces

MCP

Model Context Protocol

Two-way, standard, discoverable

ART as MCP server

Exposes agent's artifacts as MCP tool for standard agentic integration

ART as MCP client

Discovers and invokes tools exposed by external MCP servers, bringing third-party agents and data into ART flows.

API

Direct tool call

Fast integration, no MCP required

Integrate agents as a tools

Seamless 3rd party integration through workflow designer

Mapped to ART's data model

No data model enforcement; results flow straight back into the orchestration.

Full data sovereignty — Run entirely with local/on-prem models: no data leaves your environment, complete privacy by design.



Copyright © 2025 HCLTech | Confidential

HCLTech

Classification: Internal

ART: Hundreds of containerized microservices that turn telco and network data into real-time insight and action.

Modular, real-time analytics platform for telco — one engine, many use cases

Powers and enhance telco use cases: Autonomous network · Fraud Risk Management · Real-time Risk Scoring · Scam Call Detection · Voice Firewall

1. Workflow Engine
2. Query Engine
3. AI / ML Engine
4. Analytics Dashboards
5. Agentic Orchestrator



Workflow engine orchestrates every stage — query, machine learning, dashboards and GenAI — across any data source (Vertica, Oracle, Impala, BigQuery, Snowflake, JDBC). Deployable on-prem, in cloud or as SaaS.

Copyright © 2025 HCLTech | Confidential

HCLTech

Security

04



GenAI Adoption Challenges: Security

Trusted AI adoption requires controlled actions, protected data, auditability and AI-powered defense

AI Manipulation

AI systems can be manipulated through prompts, tool invocation or autonomous agent behaviors, leading to unintended or unauthorized actions

Data Leakage

AI adoption can expose sensitive information if data boundaries, tenant isolation and customer environments are not properly controlled.

Accountability & Auditability

AI decisions and actions must remain explainable, approved and traceable, especially when they affect enterprise or network-facing processes

AI Driven Frauds

Attackers can use AI to accelerate scams, fraud patterns, deepfakes and behavioral deception.

Copyright © 2025 HCLTech | Confidential

Classification: Internal

A secure AI for a secure Enterprise

Security AI Framework

Prompt guardrails
Tool guardrails
Human In the Loop
Audit Trail
Data Boundaries

Security AI Engine

Cyber Agents Attacks
SCAM Detection
Deepfake Detection
Behavioral analysis
Application hardening

CTG framework for AI Security



Copyright © 2025 HCLTech | Confidential
HCLTech

HCL Tech for AI in Telco

Turning AI capabilities into vertical, profitable and secure CSP value streams.



Autonomous Operations

AI that predicts and executes safely, supported by Specialized Sovereign Models (SLM)



Product & Services Transformation

AI that helps modernize Network Applications, owning the Software Development Lifecycle



New Revenue Streams

AI that moves from cost efficiency to direct revenue generation and customer trust improvement



Protection

AI that defends against "machine-speed" cyber attacks: Frauds, Phishing, Scam, Spam

Engineering & Advisory Competence

HCLTech | Supercharging Progress™

Thank you



Revenue Intelligence User Forum – 2026