Revista ft

www.revistaft.com.br

Arquitetura de sistemas multiagentes para integração segura de dados em ambientes industriais com múltiplas camadas de criptografia

Multi-agent system architecture for secure data integration in industrial environments with multiple encryption layers

Holden Offmenn [1]
Ítala Lorena de Lima Ferreira [2]
Daniely Dantas Lobato [3]
Jhônatas Cardoso Luz [4]
Luana Dalla Rosa de Carvalho [5]
Laís Miranda Olímpio[6]
André Luiz Samistraro Santin[7]

Resumo

A integração de dados industriais em larga escala na cadeia produtiva de telecomunicações enfrenta gargalos críticos devido à fragmentação em silos heterogêneos e restrições de segurança que impõem até sete camadas de criptografia. Este artigo descreve o desenvolvimento e a validação de uma arquitetura de software, denominada Cyber Nexus, projetada para otimizar a Análise de Causa Raiz (RCA). O objetivo central foi reduzir a latência de acesso e processamento de dados por meio de uma arquitetura descentralizada de Sistemas Multiagentes (MAS) orquestrados por Modelos de Linguagem de Grande Escala (LLMs). A metodologia empregada foi o desenvolvimento experimental, utilizando uma abordagem híbrida que combinou práticas do PMBOK® para governança e o framework Scrum para execução iterativa. A solução foi implementada com microsserviços em FastAPI, utilizando técnicas de *Retrieval-Augmented Generation* (RAG) "in-loco" para evitar a centralização em *Data Lakes* tradicionais, preservando o sigilo industrial. Os resultados experimentais validaram a eficácia da solução, alcançando uma redução de 90% na latência de leitura via *stream* e garantindo a integridade dos dados através de um "Firewall Semântico" com *Guardrails* ativos. Conclui-se que a arquitetura proposta estabelece um novo paradigma de interoperabilidade segura para a Indústria 4.0.

Palavras-chave: Sistemas Multiagentes. LLM. Indústria 4.0. Segurança Cibernética. Integração de Dados.

Abstract

Large-scale industrial data integration within the telecommunications production chain faces critical bottlenecks due to fragmentation across heterogeneous silos and security constraints that impose up to

[1] Especialista em Inteligência Artificial do Instituto Conecthus. e-mail: holden.offmenn@conecthus.org.br
[2] Cientista de Dados do Instituto Conecthus. e-mail: itala.ferreira@conecthus.org.br
[3] Cientista de Dados do Instituto Conecthus. e-mail: daniely.lobato@conecthus.org.br
[4] Desenvolvedor Back-End do Instituto Conecthus. e-mail: jhonatas.luz@conecthus.org.br
[5] Analista de Testes do Instituto Conecthus. e-mail: luana.carvalho@conecthus.org.br
[6] Gerente de Negócios da Huawei. e-mail: lais.olimpio@huawei.com
[7] Gerente de Pesquisa e Desenvolvimento da Huawei. e-mail: andre.santin@huawei.com

seven layers of encryption. This article describes the development and validation of a software architecture, called Cyber Nexus, designed to optimize Root Cause Analysis (RCA). The main objective was to reduce data access and processing latency through a decentralized Multi-Agent Systems (MAS) architecture orchestrated by Large Language Models (LLMs). The methodology employed was experimental development, using a hybrid approach that combined PMBOK® practices for governance and the Scrum framework for iterative execution. The solution was implemented with microservices in FastAPI, using in-loco Retrieval-Augmented Generation (RAG) techniques to avoid centralization in traditional Data Lakes, thus preserving industrial confidentiality. The experimental results validated the effectiveness of the solution, achieving a 90% reduction in stream-reading latency and ensuring data integrity through a Semantic Firewall with active guardrails. It is concluded that the proposed architecture establishes a new paradigm of secure interoperability for Industry 4.0.

Keywords: Multi-Agent Systems. LLM. Industry 4.0. Cybersecurity. Data Integration.

1 INTRODUÇÃO

A ascensão da Indústria 4.0 consolidou a integração de sistemas ciber-físicos e a inteligência artificial como pilares fundamentais para a modernização fabril. Segundo Vogel-Heuser e Seitz (2025), a adoção de Sistemas Multiagentes (MAS) é essencial para garantir a interoperabilidade semântica entre as camadas da arquitetura RAMI 4.0, permitindo que ativos de produção operem com altos níveis de autonomia e sociabilidade. Entretanto, a aplicação prática dessas tecnologias em ambientes de manufatura de alta escala enfrenta o desafio crítico dos silos de dados heterogêneos e das rigorosas restrições de segurança cibernética (CHKIRBENE et al., 2025).

No contexto da fabricação de dispositivos de telecomunicações da Huawei em Manaus, o processo de Análise de Causa Raiz (RCA) destaca-se como um gargalo operacional. Atualmente, a identificação de falhas complexas em produtos como a família OptiXstar exige o cruzamento manual de dados provenientes do sistema Oracle (QualitySys), logs de servidores Linux e bases proprietárias AICC/PLM, resultando em ciclos de análise que variam de 4 a 15 dias. Essa latência é agravada pela necessidade de conformidade com até sete camadas de criptografia e restrições geopolíticas que inviabilizam o uso de infraestruturas de nuvem pública (Google, AWS ou Azure).

Estudos recentes demonstram que Modelos de Linguagem de Grande Escala (LLMs) podem transformar a RCA em uma tarefa generativa, alcançando alta precisão na identificação de falhas a partir de logs e relatórios técnicos (MDPI, 2024). A utilização de

técnicas como o Retrieval-Augmented Generation (RAG) permite que esses modelos acessem bases de conhecimento dinâmicas sem a necessidade de re-treinamento constante (TRAN et al., 2026). Contudo, a aplicação dessas técnicas em hardware sensível exige abordagens que protejam a informação através de protocolos de Security by Design e criptografia híbrida (VINOD; SUBAPRIYA, 2025).

Diante deste cenário, o projeto Cyber Nexus propõe uma arquitetura descentralizada de sistemas multiagentes orquestrados por LLMs — especificamente o modelo nacional Maritaca AI e o modelo DeepSeek — para realizar a integração segura e a análise preditiva "na borda". A hipótese central deste trabalho é que a orquestração de agentes especializados pode reduzir a latência de acesso aos dados em até 90% e o ciclo total de RCA para menos de 48 horas, preservando a integridade das múltiplas camadas de criptografia exigidas pela infraestrutura industrial proprietária.

O objetivo deste artigo é descrever o desenvolvimento e a validação dessa arquitetura, elevando a solução ao nível de maturidade tecnológica TRL 6 através de testes experimentais em ambiente relevante.

2 FUNDAMENTAÇÃO TEÓRICA OU REVISÃO DA LITERATURA

A base conceitual deste trabalho repousa sobre a convergência entre a autonomia de agentes, o poder de processamento semântico dos Modelos de Linguagem de Grande Escala (LLMs) e a necessidade de segurança em arquiteturas industriais complexas.

2.1 Sistemas Multiagentes (MAS) na Indústria 4.0

A utilização de Sistemas Multiagentes é uma das estratégias mais eficazes para lidar com a descentralização exigida pela Indústria 4.0. Segundo Vogel-Heuser e Seitz (2025), um agente é um sistema computacional capaz de ação autônoma em um ambiente para atingir seus objetivos de design. Na manufatura, os MAS permitem a interoperabilidade entre silos de dados, onde cada agente é responsável por uma tarefa específica — como extração ou monitoramento — facilitando a orquestração de processos heterogêneos sem a necessidade de uma governança centralizada rígida.

2.2 Modelos de Linguagem de Grande Escala (LLMs) e RAG

Os LLMs emergiram como ferramentas poderosas para a interpretação de dados não estruturados e logs técnicos. Chkirbene et al. (2025) destacam que modelos federados ou adaptados localmente são essenciais para manter a soberania dos dados em setores estratégicos. A técnica de *Retrieval-Augmented Generation* (RAG) complementa os LLMs ao permitir que o modelo acesse documentos externos em tempo real para fundamentar suas respostas. No contexto de RCA, essa abordagem é superior ao *fine-tuning* tradicional, pois garante que a análise seja baseada no estado atualizado da linha de produção (TRAN et al., 2026).

2.3 Análise de Causa Raiz (RCA) e Segurança Cibernética

A Análise de Causa Raiz em hardware de alta complexidade envolve a identificação de correlações não óbvias entre variáveis de teste e falhas de campo. Estudos recentes (MDPI, 2024; ARXIV, 2025) indicam que a automação da RCA via IA pode reduzir drasticamente o tempo de diagnóstico, especialmente quando integrada a sistemas de telemetria.

Entretanto, a integridade dessa análise depende da segurança no tráfego das informações. Em ambientes industriais com múltiplas camadas de criptografia, a implementação de protocolos de *Security by Design* é mandatória. Conforme Vinod e Subapriya (2025), a criptografia híbrida e o controle granular de acesso através de APIs são necessários para proteger segredos industriais enquanto se permite a visibilidade necessária para a inteligência de dados.

3 METODOLOGIA

A metodologia adotada neste trabalho fundamenta-se no desenvolvimento experimental e na pesquisa aplicada, estruturada para transpor os desafios de interoperabilidade e segurança em um ambiente de manufatura de alta complexidade. O percurso metodológico foi dividido em dimensões de gestão, arquitetura técnica e validação experimental.

3.1 Enquadramento e Procedimentos de Gestão

A pesquisa seguiu uma abordagem qualitativa quanto à análise dos requisitos e quantitativa no que tange à validação de performance. A gestão do projeto utilizou um modelo híbrido: as diretrizes do **PMBOK®** garantiram a governança de riscos, custos e o alinhamento estratégico com os padrões da Indústria 4.0. Simultaneamente, o framework **SCRUM** foi

empregado para a execução técnica, organizando o desenvolvimento em ciclos iterativos (Sprints) que permitiram a entrega contínua de incrementos funcionais e o ajuste rápido frente a impedimentos técnicos de rede e segurança.

3.2 Arquitetura de Sistemas Multiagentes (MAS)

A arquitetura proposta, denominada Cyber Nexus, foi desenvolvida para operar como um ecossistema de agentes autônomos e especializados, orquestrados por Modelos de Linguagem de Grande Escala (LLMs). A implementação técnica utilizou o framework FastAPI para a criação de microsserviços conteinerizados em Docker, garantindo escalabilidade e isolamento. A solução Cyber Nexus foi concebida sob uma arquitetura de microsserviços descentralizada para evitar a criação de um ponto único de falha ou de vulnerabilidade. A implementação técnica baseou-se nos seguintes pilares:

- **Orquestração Agentic**: Utilizou-se o framework LangChain para gerenciar o "Agentic Loop", permitindo que os agentes tomassem decisões autônomas sobre qual ferramenta (tool) acionar para resolver uma consulta de Causa Raiz.
- **Stack Tecnológica**: Os agentes foram desenvolvidos em Python, utilizando FastAPI para a exposição de interfaces de comunicação e Docker para a conteinerização dos serviços, garantindo portabilidade entre os servidores Ubuntu da planta industrial.
- **Modelos de Linguagem (LLMs)**: A inteligência central foi composta de forma híbrida pelo modelo nacional Maritaca AI (otimizado para o português técnico) e pelo modelo DeepSeek, avaliados por sua capacidade de interpretar logs complexos e estruturas de bancos de dados relacionais.

3.3 Estratégia de Integração e Segurança *by Design*

Dada a restrição de até sete camadas de criptografia (C1 a C7) na infraestrutura proprietária, a metodologia de integração não utilizou a extração massiva de dados (ETL tradicional). Em vez disso:

- **RAG Distribuído**: Implementou-se o *Retrieval-Augmented Generation* diretamente nas fontes. Agentes especializados realizam conexões via SSH para leitura de logs em tempo real e via drivers Oracle para consulta ao sistema *QualitySys*.
- **Segurança Transversal**: A comunicação entre agentes foi protegida por protocolos mTLS (Mutual TLS). Além disso, inseriu-se uma camada de Guardrails e um

"Firewall Semântico" para monitorar as interações das LLMs, garantindo que nenhum dado sensível ou segredo industrial ultrapassasse os limites da rede controlada.

- **Resiliência**: Para evitar loops infinitos de processamento (gargalo comum em MAS), estabeleceu-se um limite de iterações (*max_iterations*) e uma estratégia de *Human-in-the-Loop* para casos de ambiguidade nos dados.

3.4 Fases do Desenvolvimento Experimental

O desenvolvimento foi segmentado em quatro etapas principais:

1. **Levantamento e Mapeamento**: Identificação das bases heterogêneas e protocolos de acesso aos sistemas de rádio frequência 5G e redes Mesh.
2. **Desenvolvimento do Motor Algorítmico**: Codificação dos agentes de extração, tratamento e análise semântica.
3. **Provas de Conceito (PoC)**: Testes em ambiente simulado para validar a redução de latência e a eficácia da criptografia.
4. **Validação em Ambiente Relevante (TRL 6)**: Execução de Testes de Aceitação do Usuário (UAT) com engenheiros da Huawei e Foxconn, utilizando dados reais de produção para cruzar falhas de campo com variáveis de calibração

3.5 Métricas de Avaliação

A eficácia da metodologia foi aferida comparando-se o modelo anterior (manual e centralizado) com a arquitetura Cyber Nexus, focando em:

- **Latência de Acesso**: Redução percentual no tempo de resposta para consultas complexas.
- **Tempo de RCA**: Redução do ciclo total de análise de causa raiz de dias para horas.
- **Precisão de Detecção**: Taxa de acerto na identificação de anomalias e padrões de falha (meta estabelecida em > 80%).

4 RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

Os resultados obtidos com a validação da arquitetura Cyber Nexus em ambiente industrial demonstram a eficácia da abordagem de sistemas multiagentes na superação de silos de dados altamente protegidos. A análise foi segmentada em métricas de performance técnica e impacto no processo de diagnóstico.

4.1 Performance de Integração e Latência

A transição do método tradicional de extração em lote (*batch*) para a leitura via *stream* descentralizada resultou em uma redução de 90% na latência de acesso aos metadados. Enquanto o processo anterior de consolidação de logs e variáveis de calibração consumia horas de processamento manual, a arquitetura de agentes orquestrados por LLM permitiu que consultas complexas, cruzando dados do QualitySys (Oracle) e logs de produção (SSH), fossem retornadas em um tempo médio inferior a 12 segundos.

Esta performance é atribuída à eficiência do framework FastAPI e à capacidade dos agentes de realizar a filtragem semântica na fonte, transmitindo apenas as informações relevantes para a análise de causa raiz, o que minimizou o tráfego em rede e a sobrecarga nos bancos de dados legados.

4.2 Impacto no Ciclo de Análise de Causa Raiz (RCA)

O ganho operacional mais expressivo foi observado na redução do ciclo total de RCA para a família de produtos OptiXstar. O tempo médio de diagnóstico, que anteriormente oscilava entre 4 e 15 dias devido à fragmentação informacional, foi reduzido para menos de 48 horas após a implementação do motor algorítmico.

A precisão dos modelos Maritaca AI e DeepSeek na identificação de anomalias e padrões de falha superou a meta estabelecida, alcançando um índice de acerto superior a 80% nos testes de validação. Os engenheiros de qualidade relataram que a capacidade da IA de correlacionar logs de rádio frequência 5G com falhas de montagem física permitiu ações corretivas preventivas na linha da Foxconn antes da ocorrência de lotes defeituosos.

4.3 Eficácia da Segurança e Confiabilidade

A arquitetura de segurança descentralizada validou a hipótese de que é possível integrar dados em ambientes com até sete camadas de criptografia sem comprometer o sigilo industrial. O "Firewall Semântico" implementado com *Guardrails* bloqueou com sucesso 100% das tentativas de extração de dados sensíveis (PII) ou segredos de projeto durante a fase de testes, garantindo a conformidade total com a LGPD e os padrões globais da Huawei.

Entretanto, durante os testes experimentais, identificou-se o desafio do *Agentic Loop* (iterações infinitas da IA em consultas ambíguas). Este ponto foi mitigado com a implementação de um limite mandatório de três iterações no LangChain e a inserção da estratégia *Human-in-the-Loop*, onde o sistema solicita clarificação ao usuário em vez de travar o processamento.

4.4 Discussão

A análise dos resultados evidencia que a arquitetura Cyber Nexus logrou êxito em equilibrar dois vetores frequentemente antagônicos em ambientes industriais: a segurança rigorosa da informação e a agilidade no processamento de dados. A redução de 90% na latência de acesso, comparada aos métodos de extração em lote (*batch*) utilizados anteriormente, confirma a eficácia da descentralização proposta pelos sistemas multiagentes.

Diferente das arquiteturas de *Big Data* convencionais, que buscam a centralização em *Data Lakes*, o Cyber Nexus validou a viabilidade do paradigma de "Inteligência na Borda" (*Edge Intelligence*). Ao levar o processamento semântico até o dado por meio de agentes especializados, a solução mitigou o impacto das sete camadas de criptografia que, em fluxos de integração tradicionais, atuariam como barreiras intransponíveis ou geradoras de latência excessiva.

A integração do modelo nacional Maritaca AI revelou-se um diferencial estratégico. Além de garantir a soberania tecnológica, a LLM demonstrou alta acurácia na interpretação de termos técnicos e logs específicos da infraestrutura da Huawei, superando desafios de barreiras linguísticas e geopolíticas que limitam o uso de soluções de nuvem de mercado. A precisão superior a 80% na detecção de anomalias valida o uso de LLMs não apenas como interfaces de conversação, mas como motores de inferência lógica para a Indústria 4.0.

Contudo, a ocorrência de *Agentic Loops* durante a fase experimental aponta para uma limitação inerente aos sistemas autônomos baseados em modelos probabilísticos. A solução de implementar uma estratégia de *Human-in-the-Loop* reforça que, embora a IA possa reduzir o ciclo de RCA de 15 dias para menos de 48 horas, o papel do engenheiro de qualidade permanece central para a validação final de diagnósticos ambíguos.

Por fim, a elevação da maturidade tecnológica para o nível TRL 6 consolida a arquitetura como um "programa de computador com inovação científica". O Cyber Nexus não apenas resolve um problema imediato de eficiência operacional, mas estabelece uma base modular e escalável que prepara o terreno para a futura evolução rumo ao Nível 6 de maturidade da Indústria 4.0 (Adaptabilidade).

5 CONCLUSÃO/CONSIDERAÇÕES FINAIS

O desenvolvimento do projeto Cyber Nexus demonstrou a viabilidade técnica da utilização de Sistemas Multiagentes (MAS) orquestrados por Modelos de Linguagem de Grande Escala (LLMs) para a superação de silos informacionais em ambientes de manufatura avançada. A implementação de uma arquitetura descentralizada permitiu a integração de bases de dados heterogêneas, como o sistema QualitySys e servidores de logs de produção, sem a necessidade de uma centralização onerosa em *Data Lakes*. Esta abordagem "in-loco" provou ser essencial para contornar as restrições geopolíticas e técnicas que limitam o uso de infraestruturas de nuvem pública, garantindo a soberania tecnológica e a conformidade com padrões proprietários.

Os resultados experimentais validaram a hipótese central do estudo, apresentando ganhos de eficiência significativos tanto na camada técnica quanto na operacional. A redução de 90% na latência de acesso aos metadados e a capacidade de processar consultas complexas em menos de 12 segundos representam um avanço crítico na gestão da informação fabril. Mais notavelmente, a automação da correlação de dados permitiu que o ciclo de Análise de Causa Raiz (RCA), que anteriormente exigia processos manuais exaustivos de até 15 dias, fosse reduzido para menos de 48 horas.

No que concerne à segurança cibernética, o Cyber Nexus estabeleceu um paradigma de *Security by Design* capaz de operar de forma íntegra sob sete camadas de criptografia proprietária. A utilização de protocolos mTLS e a implementação de um "Firewall Semântico" com *Guardrails* ativos asseguraram que o processamento realizado pelas LLMs ocorresse sem o risco de vazamento de segredos industriais ou dados sensíveis. Esta camada de proteção transversal foi determinante para garantir a integridade e a confidencialidade das informações em um ambiente de conformidade técnica rigorosa.

A conclusão bem-sucedida das etapas de desenvolvimento experimental permitiu elevar a maturidade tecnológica da solução para o nível TRL 6. O motor algorítmico foi validado em ambiente relevante, demonstrando uma precisão superior a 80% na detecção de anomalias e na identificação de padrões de falha em equipamentos de rádio frequência 5G e redes Mesh. Esta validação consolida o projeto não apenas como um avanço em engenharia de software, mas como uma infraestrutura robusta para a aplicação prática de inteligência artificial generativa no contexto da Indústria 4.0.

Como perspetiva para trabalhos futuros, recomenda-se a expansão da arquitetura para atingir níveis de maturidade superiores (TRL 7 e 8), integrando o Cyber Nexus diretamente

nos fluxos de suporte à decisão autônoma (Nível 6 de maturidade industrial). Sugere-se ainda o aprimoramento dos mecanismos de mitigação de *Agentic Loops* através de modelos de recompensa específicos para contextos industriais e a exploração da escalabilidade desta solução para outros setores do Polo Industrial de Manaus. Em última análise, o projeto reafirma a capacidade de gerar inovação de alto impacto e competitividade global a partir do ecossistema tecnológico regional.

REFERÊNCIAS

ARXIV. **Towards LLM-based Root Cause Analysis of Hardware Design Failures**. arXiv, 2025. Disponível em: https://arxiv.org/html/2507.06512v1. Acesso em: 15 mar. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, ago. 2018.

CHKIRBENE, Z. et al. **A Review of Federated Large Language Models for Industry 4.0**. MDPI Sensors, v. 26, n. 4, p. 1116, 2025. Disponível em: https://www.mdpi.com/1424-8220/26/4/1116. Acesso em: 12 mar. 2026.

DOCKER. **Docker Documentation**. 2025. Disponível em: https://docs.docker.com/. Acesso em: 10 mar. 2026.

FASTAPI. **FastAPI Documentation**. 2025. Disponível em: https://fastapi.tiangolo.com/. Acesso em: 10 mar. 2026.

LANGCHAIN. **LangChain Documentation**. 2025. Disponível em: https://python.langchain.com/. Acesso em: 10 mar. 2026.

MARITACA AI. **Maritaca AI: Modelos de Linguagem para o Contexto Brasileiro**. 2025. Disponível em: https://www.maritaca.ai/. Acesso em: 12 mar. 2026.

MDPI. **RCEGen: A Generative Approach for Automated Root Cause Analysis Using Large Language Models (LLMs)**. MDPI Electronics, v. 4, n. 4, p. 29, 2024. Disponível em: https://www.mdpi.com/2674-113X/4/4/29. Acesso em: 14 mar. 2026.

PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project Management Body of Knowledge (PMBOK® Guide)**. 7. ed. Pennsylvania: PMI, 2021.

SCHWABER, K.; SUTHERLAND, J. **The Scrum Guide**. 2020. Disponível em: https://scrumguides.org/. Acesso em: 05 mar. 2026.

TRAN, N. P. et al. **LLM-Augmented Knowledge Base Construction for Root Cause Analysis**. IEEE Xplore, 2026. Disponível em: https://ieeexplore.ieee.org/document/11366685. Acesso em: 16 mar. 2026.

VINOD, D.; SUBAPRIYA, V. **Security in Industrial IoT: Mixed Encryption**. ResearchGate, 2025. Disponível em: https://www.researchgate.net/publication/326954520_Challenges_of_Securing_the_Industrial_Internet_of_Things_Value_Chain. Acesso em: 11 mar. 2026.

VOGEL-HEUSER, B.; SEITZ, M. **Multi-agent systems to enable Industry 4.0**. Semantic Scholar, 2025. Disponível em: https://www.degruyterbrill.com/document/doi/10.1515/auto-2020-0004/html. Acesso em: 13 mar. 2026.