Proposta de Arquitetura em FPGA para Gateway Unidirecional Seguro em Coletores Industriais

Domingos Sávio Faria Paes[1], **Otávio de Souza Martins Gomes**[1]
Tales Cléber Pimenta[1], **Robson Luiz Moreno**[1]

[1] Instituto de Engenharia de Sistemas e Tecnologia da Informação
Universidade Federal de Itajubá (UNIFEI)
Caixa Postal: 50 – CEP 37.500-903 – Itajubá – MG – Brasil

{domingospaes, otavio.gomes, tales, moreno}@unifei.edu.br

Abstract. *This paper investigates the feasibility of an FPGA-based data diode architecture for a secure unidirectional gateway integrated with industrial data collectors, aiming to enable controlled data transfer between OT and IT networks. The proposal is positioned at level 3.5 of the Purdue model and acts as a selective boundary filter, forwarding only consolidated data, telemetry, alarms, and events, while keeping real-time control traffic confined to the OT domain. The architecture is organized into functional blocks for Ethernet reception, protocol parsing and classification, security policy enforcement, normalization, and unidirectional transmission, coordinated by a finite state machine. As the prototype is still under development, the study focuses on architectural modeling and feasibility analysis.*

Resumo. *Este artigo investiga a viabilidade de uma arquitetura de diodo de dados em FPGA para um gateway unidirecional seguro integrado a coletores industriais, com o objetivo de permitir a transferência controlada de dados entre redes OT e IT. A proposta é posicionada na camada 3.5 do modelo Purdue e atua como um filtro seletivo de fronteira, encaminhando apenas dados consolidados, telemetria, alarmes e eventos, enquanto restringe o tráfego de controle em tempo real ao domínio OT. A arquitetura é estruturada em blocos funcionais de recepção Ethernet, parsing e classificação de protocolos, aplicação de política de segurança, normalização e transmissão unidirecional, coordenados por uma máquina de estados finitos. Como o protótipo ainda está em fase de elaboração, o trabalho concentra-se na modelagem arquitetural e na análise de viabilidade.*

1. Introdução

Na era da Indústria 4.0, a integração entre ativos industriais e sistemas corporativos ampliou a superfície de ataque e elevou os riscos associados à conexão entre OT e IT [Monostori et al. 2016]. Nesse cenário, a popularização da Inteligência Artificial também fortaleceu atacantes ao facilitar novas táticas, técnicas e processos além de criar um novo modelo de negócio, o *Cybercrime-as-a-Service* (CaaS) [Labs 2025].

Por isso, dados de sensores, atuadores e máquinas devem trafegar entre OT e IT com isolamento rigoroso de zonas e condutos, alinhado às normas ISA/IEC 62443 e NIST

SP 800-82 [Commission et al. 2020, Stouffer et al. 2023]. Uma solução eficaz é o uso de *Gateways* Unidirecionais Seguros (*Unidirectional Security Gateways* – USG) baseados em FPGA, capazes de impor unidirecionalidade física ao canal de dados eliminando o caminho de retorno ao ambiente operacional [Ha et al. 2023].

Além de reforçar a segurança, a implementação em FPGA reduz a necessidade de *hardware* adicional e permite processamento em tempo real, com baixa latência, o que é essencial em aplicações industriais sensíveis. Com isso, torna-se possível integrar sistemas industriais baseados em ethernet à indústria 4.0 disponibilizando dados de processo, por exemplo, para manutenção preditiva e análise de anomalias, sem introduzir riscos de acesso externo ao sistema monitorado.

Assim, este trabalho investiga a integração de USG (*Unidirectional Security Gateways*) com coletores industriais na camada limite OT do modelo Purdue [Williams 1994]. Diferente de soluções da literatura baseadas em *software*, que geram latências imprevisíveis, ou em *hardware* restritas a protocolos seriais legados, a arquitetura proposta inova ao aliar o isolamento físico da FPGA ao *parsing* de protocolos Ethernet modernos. Ao impor determinismo à filtragem seletiva de *payloads*, a solução preenche a lacuna entre a segurança rígida de *hardware* e a flexibilidade exigida pelas infraestruturas industriais atuais.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados, a Seção 3 descreve a arquitetura proposta, a Seção 4 detalha a metodologia adotada, a Seção 5 discute a proposta e suas limitações, e a Seção 6 apresenta as conclusões.

2. Trabalhos Relacionados

Os trabalhos relacionados podem ser agrupados em diodos de dados tradicionais, *gateways* unidirecionais seguros e soluções baseadas em FPGA. Em conjunto, essa literatura mostra a evolução de mecanismos de isolamento físico simples para arquiteturas mais flexíveis, capazes de inspecionar e filtrar tráfego em *hardware*.

2.1. Diodos de dados tradicionais

Os primeiros diodos de dados foram propostos para garantir isolamento unidirecional em ambientes militares e de alta segurança, com forte dependência de separação física e uso restrito a fluxos em um único sentido [Cohen 1988]. Em cenários industriais, porém, essa abordagem é limitada por não lidar bem com protocolos que exigem sessão, confirmação ou troca bidirecional.

2.2. *Gateways* unidirecionais seguros

A evolução desses dispositivos levou aos USGs, que preservam a unidirecionalidade física e acrescentam mecanismos de camada superior para suportar protocolos mais complexos [Gaina et al. 2024]. Assim, tornam-se mais adequados à integração entre OT e IT em ICS e SCADA, especialmente quando o objetivo é expor dados operacionais sem comprometer o ambiente protegido.

2.3. Soluções baseadas em FPGA

O uso de FPGA como núcleo de segurança tem se destacado por permitir a implementação direta da lógica unidirecional em *hardware*, com baixa latência e maior controle so-

bre o fluxo de pacotes [Ha et al. 2023]. Além disso, sua reconfigurabilidade favorece a adaptação a novas políticas e protocolos sem substituição completa do *hardware*.

3. Arquitetura Proposta

A solução proposta consiste em um *gateway* unidirecional seguro implementado em FPGA, integrado a um coletor de dados industriais para permitir a transferência controlada de informações entre a rede OT e a rede IT.

A arquitetura foi concebida de forma independente de *hardware* específico, com prototipação futura prevista para a placa Terasic DE25-Standard, em conjunto com a expansão Ethernet HSMC. Esse arranjo prevê duas interfaces físicas distintas: uma voltada à OT e outra à IT, à internet ou à nuvem.

O caminho de dados utiliza o bloco Altera Triple-Speed Ethernet (TSE) IP Core [Corporation 2025] associado ao bloco IP TOE (*TCP Offload Engine*)[Wang et al. 2025], os quais são responsáveis pelo processamento das camadas MAC e PHY, além do gerenciamento das sessões TCP. A terminação das conexões TCP e a extração do *payload* são realizadas por uma máquina de estados no núcleo do FPGA, eliminando dependências de *software* no caminho principal.

Do ponto de vista funcional, a Figura 1 mostra como a arquitetura foi organizada em cinco blocos principais: recepção Ethernet, *parser*/classificador de protocolos, motor de política de segurança, módulo de normalização e *buffer* unidirecional, e transmissão ethernet. Essa divisão facilita a implementação em *hardware*, reduz a complexidade do fluxo de dados e permite que o FPGA concentre a lógica crítica de segurança, eliminando dependências de *software* no caminho principal da transmissão.

As politicas de segurança são armazenadas em memória *flash* interna e podem ser modificadas através da interface de configuração ligada ao HPS (*Hard Processor System*) fora do fluxo segurança, assim não comprometendo o caminho crítico.

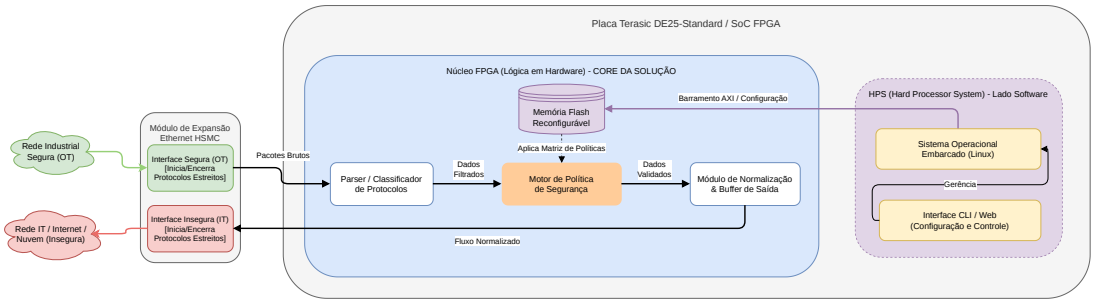

Figura 1. Núcleo FPGA

A FSM, apresentada na Figura 2, opera em três regimes: encaminhamento autorizado, descarte por política e tratamento de erro. Quando o tráfego não é autorizado ou o *parsing* falha, o pacote é descartado e o sistema retorna ao estado inicial.

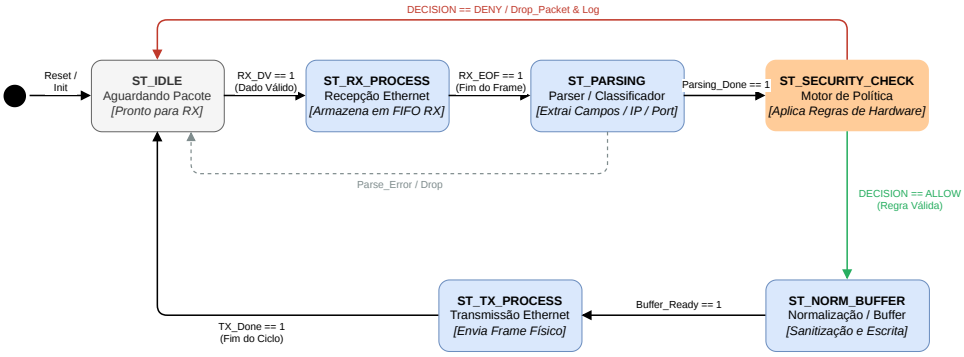

Figura 2. FSM - Máquina de Estados Finitos

A máquina de estados finitos ou apenas FSM (*Finite State Machine*) seleciona apenas dados úteis para supervisão e integração com a IT, como telemetria, eventos e alarmes, enquanto descarta mensagens de controle em tempo real, pacotes corrompidos e protocolos não reconhecidos. A Figura 3 posiciona o *gateway* na camada 3.5 do modelo Purdue, onde atua como elemento de borda entre OT e IT, preservando o isolamento industrial e reduzindo a superfície de ataque.

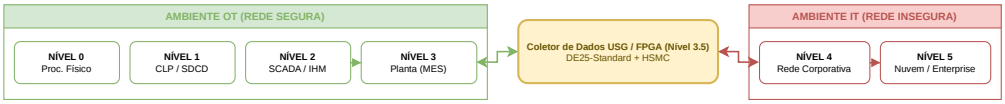

Figura 3. Modelo Purdue com posicionamento do USG/FPGA

4. Metodologia

A metodologia adotada neste trabalho é de natureza propositiva, descritiva e analítica, tendo como objetivo investigar a viabilidade de um *gateway* unidirecional seguro baseado em FPGA (*Field Programmable Gate Array*) para integração entre redes OT e IT. Como não há implementação física ou protótipo funcional nesta etapa, o estudo concentra-se na definição dos requisitos do sistema, na modelagem da arquitetura proposta, na análise conceitual do tratamento dos protocolos industriais e na avaliação de sua coerência com boas práticas de segmentação e segurança em ambientes industriais.

A primeira etapa consistiu na delimitação do problema de pesquisa, a partir da identificação do aumento da superfície de ataque decorrente da integração entre redes operacionais e corporativas em ambientes de Indústria 4.0. Com base nesse contexto, foram definidos os requisitos centrais da solução: unidirecionalidade física do fluxo de dados, separação entre interface segura e interface insegura, filtragem seletiva do tráfego industrial e suporte a protocolos relevantes para a fronteira OT/IT.

Na segunda etapa, foi realizada a modelagem funcional da arquitetura, considerando o posicionamento do dispositivo na camada 3.5 do modelo Purdue. Essa escolha decorre do fato de que a solução não foi concebida para transportar o tráfego bruto do chão de fábrica, mas para atuar como um elemento de fronteira entre a supervisão industrial e a rede corporativa, permitindo apenas a exposição controlada de dados com valor informacional para a TI.

O sistema foi então estruturado em blocos lógicos de recepção, *parsing*, verificação de segurança, normalização e transmissão, organizados sob o controle de uma FSM responsável por coordenar os fluxos válidos, os descartes por política e o tratamento de erros.

A terceira etapa consistiu na análise de alguns protocolos industriais a serem considerados inicialmente pela proposta, vistos na Tabela 1. Em vez de assumir que todo o tráfego da OT deva atravessar o *gateway*, adotou-se o princípio de filtragem seletiva de fronteira, mantendo protocolos de controle em tempo real restritos à OT e permitindo a travessia apenas de protocolos de supervisão, telemetria e integração quando associados a dados agregados, alarmes e eventos.

Tabela 1. Classificação dos protocolos quanto ao tratamento na fronteira OT/IT

Protocolo	**Classificação**	**Uso principal**
PROFINET RT	Restrito à OT	Controle em tempo real
EtherCAT	Restrito à OT	Controle em tempo real
IEC 61850 GOOSE/SV	Restrito à OT	Automação elétrica em tempo real
OPC UA	OT $\rightarrow$ IT	Supervisão e interoperabilidade
MQTT	OT $\rightarrow$ IT	Telemetria e IIoT
DNP3	OT $\rightarrow$ IT	Supervisão e telemetria
IEC 61850 GOOSE/MMS	OT $\rightarrow$ IT	Supervisão e troca de dados
HTTP/HTTPS	OT $\rightarrow$ IT	Integração com serviços externos

A partir dessa classificação, foi definida a lógica de funcionamento da FSM que rege o dispositivo. No fluxo normal, o processamento segue a sequência ST_IDLE, RX, PARSE, SECURITY_CHECK, NORM e TX, retornando ao estado inicial após a transmissão. Quando o motor de política de segurança identifica tráfego não autorizado, a FSM interrompe o processamento e retorna imediatamente a ST_IDLE, descartando o pacote antes das etapas de normalização e transmissão.

Assim, a integração dos blocos funcionais mapeados estabelece a base estrutural para o funcionamento do *gateway* de segurança.

4.1. Análise de Viabilidade Operacional

A viabilidade da arquitetura proposta é validada analiticamente por meio das restrições operacionais do *hardware* e da dinâmica da FSM projetada. Embora os testes empíricos dependam de síntese final, a viabilidade de tempo real é garantida pelo determinismo do *hardware*: o *parsing* e a aplicação de políticas por FSM dedicada elimina o *overhead* e o *jitter* imprevisível em sistemas operacionais tradicionais.

Como o sistema descarta o tráfego pesado de controle, transmitindo apenas eventos e telemetria, o volume de dados na saída diminui drasticamente. Esse fator, aliado ao uso de blocos de memória RAM interna do FPGA configurados como filas FIFO para o *buffer* de saída, mitiga o risco de estouro de memória (*overflow*) inerente à unidirecionalidade do canal, comprovando a viabilidade arquitetural da solução.

5. Discussão

A proposta é coerente com o problema de segurança ao tratar a integração OT/IT como uma fronteira controlada. O posicionamento na camada 3.5 do modelo Purdue evita a

exposição direta do tráfego bruto do chão de fábrica e concentra a atuação sobre dados com valor informacional para a TI.

Sob a perspectiva funcional, o *gateway* atua como filtro seletivo de fronteira. Protocolos de controle em tempo real permanecem restritos à OT, enquanto protocolos de supervisão e telemetria podem atravessar a fronteira quando associados a dados consolidados.

Do ponto de vista da segurança, o uso de FPGA concentra em *hardware* funções críticas de *parsing*, política e encaminhamento, reduzindo a dependência de *software*. A organização da FSM em caminhos de sucesso, descarte e erro também aumenta a robustez do dispositivo.

A principal contribuição desta proposta está na combinação entre um coletor industrial, filtragem seletiva por protocolo e implementação das funções críticas em FPGA, de modo a expor apenas dados com valor de supervisão e manter tráfego de controle e fluxos inválidos restritos à OT. A arquitetura é coerente e conceitualmente sólida, tendo sua validação experimental expandida em protótipo físico nas próximas etapas do projeto de forma a avaliar latência, vazão, consumo de recursos e comportamento diante de tráfego malformado ou não reconhecido. Também permanece relevante verificar o tratamento de protocolos que dependem de sessão ou de serviços intermediários, como *broker* e *proxy*, o que reforça a necessidade de testes em cenário representativo.

6. Conclusão

Este trabalho propôs uma arquitetura de *gateway* unidirecional seguro em FPGA para transferência controlada de dados entre redes OT e IT, sem comprometer o isolamento do ambiente operacional. A proposta responde ao aumento da superfície de ataque em ambientes industriais conectados e à necessidade de disponibilizar dados de processo para supervisão e análise sem abrir caminhos de retorno para a rede OT.

A arquitetura é coerente com esse objetivo ao posicionar o dispositivo na camada 3.5 do modelo Purdue, atuando como elemento de fronteira entre OT e IT. Assim, dados como telemetria, alarmes e eventos podem atravessar a fronteira, enquanto protocolos de controle em tempo real permanecem restritos ao domínio operacional.

Do ponto de vista técnico, o uso de FPGA concentra em *hardware* funções críticas de processamento e reduz a dependência de *software*. A FSM reforça essa lógica ao separar encaminhamento autorizado, descarte por política e tratamento de erro, aumentando a robustez do sistema.

A principal contribuição do artigo está na formulação de uma arquitetura de referência para *gateways* unidirecionais seguros, articulando segmentação OT/IT, seleção de protocolos de fronteira e filtragem em *hardware*. Como trabalhos futuros, pretende-se implementar o protótipo, sintetizar a lógica em FPGA e avaliar desempenho, robustez e comportamento sob diferentes perfis de tráfego.

Agradecimentos

Este trabalho contou com o apoio da empresa de consultoria e segurança CLAVIS, por meio do projeto ”Segurança cibernética em sistemas de tecnologia operacional (Cyber OT) e infraestruturas críticas”.

Referências

Cohen, F. (1988). Designing provably correct information networks with digital diodes. *Computers & Security*, 7(3):279–286.

Commission, I. E. et al. (2020). Security for industrial automation and control systems: Part 3-2: Security risk assessment for system design. *International standard, IEC*, pages 62443–3.

Corporation, A. (2025). Triple-Speed Ethernet FPGA IP User Guide. https://docs.altera.com/r/docs/683402/25.3/triple-speed-ethernet-ip-user-guide/about-this-ip. Acessado em: 10-03-2026.

Gaina, L., Stangaciu, C. S., Stanescu, D., Gusita, B., and Micea, M. V. (2024). Unidirectional communications in secure iot systems—a survey. *Sensors*, 24(23):7528.

Ha, S. S., Beuster, H., Doebbert, T. R., and Scholl, G. (2023). An fpga-based unidirectional gateway proposal for ot-it network separation to secure industrial automation systems. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, pages 1–6. IEEE.

Labs, F. (2025). Cyberthreat Predictions for 2025. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-prediction-2025.pdf. Acessado em: 10-03-2026.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., and Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*, 65(2):621–641.

Stouffer, K., Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., et al. (2023). Guide to operational technology (ot) security. *US Department of Commerce, National Institute of Standards and Technology*.

Wang, H., Song, P., Chen, Y., Zhao, J., Zhang, H., and Han, Z. (2025). Implementation of tcp/ip protocol stack offloading based on fpga. In *Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering*, pages 225–231.

Williams, T. J. (1994). The purdue enterprise reference architecture. *Computers in industry*, 24(2-3):141–158.