

Resiliência Cibernética em Ambientes de TO: Uma Abordagem Baseada em Monitoramento Passivo em Conformidade com a IEC 62443

Carlos W. de Souza¹, Gabriel M. Rosa¹, Otávio S. M. Gomes¹

¹Instituto de Engenharia de Sistemas e Tecnologia da Informação
Universidade Federal de Itajubá (UNIFEI)
Av. BPS 1303 – 37.500-903 – Itajubá – MG – Brasil

{waldecir.souza, d2022005992, otavio.gomes}@unifei.edu.br

Abstract. *The convergence between Information Technology (IT) and Operational Technology (OT) has eliminated the air-gap isolation of industrial environments, exposing critical infrastructures to cyber threats. Unlike IT, OT environments prioritize availability and physical safety, requiring specialized defense strategies. This paper analyzes the vulnerability of Industrial Control Systems (ICS) and proposes a defense-in-depth approach based on passive monitoring and Deep Packet Inspection (DPI). Through a practical experiment using a Modbus TCP module, we demonstrate how unauthorized parameter changes can be detected and mapped to the MITRE ATT&CK for ICS framework. The results show that passive monitoring can support security objectives related to IEC 62443, particularly system integrity, without introducing additional traffic into the monitored operational path.*

Resumo. *A convergência entre TI e TO reduziu o isolamento físico das indústrias, expondo infraestruturas críticas a incidentes cibernéticos. Diferente da TI, a TO prioriza disponibilidade e segurança física de máquinas, equipamentos, meio ambiente e pessoas. Este artigo aborda vulnerabilidades em sistemas industriais e propõe uma estratégia de defesa em profundidade baseada em monitoramento passivo e DPI. Por meio de um experimento prático com o protocolo Modbus TCP, apresenta-se como alterações não autorizadas são detectadas e mapeadas para o framework MITRE ATT&CK for ICS. Os resultados indicam que o monitoramento passivo pode contribuir para objetivos de segurança relacionados à IEC 62443, especialmente à integridade dos sistemas, sem introduzir tráfego adicional no caminho operacional monitorado.*

1. Introdução

A transição para a Indústria 4.0 reduziu o isolamento físico dos ambientes industriais, expondo infraestruturas críticas a novos desafios cibernéticos. Diferente da Tecnologia da Informação (TI), onde a confidencialidade é o pilar central, a Tecnologia Operacional (TO) prioriza a disponibilidade operacional e a segurança física de seus ativos. Neste cenário, incidentes podem causar não apenas perdas financeiras, mas também danos ambientais e riscos à integridade humana. Para mitigar esses riscos e assegurar a resiliência operacional, torna-se fundamental transitar de uma postura de segurança tradicionalmente

reativa, focada apenas na contenção pós-incidente, para um modelo proativo. A visibilidade de ativos, obtida por meio do levantamento automatizado, constitui a base dessa estratégia [Knapp and Langill 2014]. Como as redes industriais evoluem de forma orgânica e frequentemente carecem de documentação atualizada, o mapeamento contínuo de dispositivos e versões de firmware permite identificar vulnerabilidades e subsidiar análises de risco.

A norma IEC 62443 estabelece que a proteção deve ser aplicada em camadas. Nesse contexto, o monitoramento passivo surge como um mecanismo técnico adequado, pois não introduz tráfego adicional no caminho operacional monitorado [Claroty 2026]. Diferente das técnicas ativas de varredura, que podem introduzir carga adicional ou, em determinados dispositivos sensíveis, causar instabilidade operacional, o monitoramento via *Deep Packet Inspection* (DPI) analisa o tráfego em tempo real por espelhamento, sem injetar pacotes na rede [Barbosa and Pras 2010].

Este trabalho apresenta uma abordagem de monitoramento passivo de redes TO baseada em DPI, combinando análise de tráfego, detecção comportamental e correlação com o MITRE ATT&CK for ICS. A abordagem é avaliada experimentalmente em um ambiente industrial controlado, no qual uma alteração não autorizada de parâmetros de rede é identificada por meio da análise integrada de capturas de pacotes e eventos observados por uma plataforma de monitoramento. Os resultados são discutidos à luz dos requisitos fundamentais da IEC 62443, avaliando-se a contribuição do monitoramento passivo para a integridade dos sistemas e a disponibilidade dos recursos.

2. Fundamentos de Segurança em Ambientes Industriais

2.1. Peculiaridades e Restrições do Ambiente de TO

Enquanto a TI é regida pela tríade CID (Confidencialidade, Integridade e Disponibilidade), o ambiente de TO inverte essas prioridades, posicionando a Disponibilidade como prioridade. Muitos ambientes industriais permanecem em operação por décadas e utilizam softwares e hardwares legados ou proprietários, cuja substituição é limitada por requisitos de disponibilidade contínua, custos de modernização e necessidade de revalidação dos processos industriais [Knapp and Langill 2014]. Esse posicionamento gera vulnerabilidades severas: ferramentas tradicionais de segurança corporativa, como antivírus baseados em agentes e varredores ativos de vulnerabilidades, são tecnicamente inviáveis devido à memória limitada dos controladores e aos rigorosos requisitos de tempo de resposta, frequentemente estabelecidos na ordem de milissegundos.

Essas características fazem com que a segurança de ambientes TO precise considerar requisitos específicos de desempenho, confiabilidade e segurança operacional [National Institute of Standards and Technology 2023].

2.2. O Modelo Purdue e os Riscos de Conectividade

O Modelo Purdue organiza a infraestrutura industrial em níveis lógicos (0 a 5), determinando que camadas distintas não devem se comunicar sem passar por zonas e conduítes de controle definidos [Williams 1994]. Os Níveis 0 a 2 abrangem dispositivos de campo e controladores, o Nível 3 reúne sistemas de supervisão e operação, enquanto os níveis superiores concentram funções corporativas e integração externa, dependendo da implementação arquitetural.

Um erro arquitetural recorrente na convergência TI/TO é conectar o Nível 4 diretamente ao Nível 2. Essa exposição direta coloca protocolos industriais clássicos, que, em sua maioria, foram concebidos sem mecanismos nativos de autenticação ou criptografia ao alcance da rede corporativa e da internet.

2.3. Estratégias de Defesa, Resiliência e o *framework* MITRE

No domínio de infraestruturas críticas, os conceitos de proteção evoluíram para o paradigma da resiliência cibernética. Enquanto a segurança convencional busca evitar que uma intrusão ocorra, a resiliência assume a premissa de que o perímetro pode ser violado. O foco se desloca para a capacidade do sistema de limitar os danos, manter a continuidade operacional mínima e recuperar-se rapidamente após o incidente, seja ele interno, externo, acidental ou intencional. A integração do monitoramento passivo ao MITRE ATT&CK for ICS permite contextualizar eventos observados segundo táticas, técnicas e procedimentos (TTPs), apoiando processos de detecção, investigação e resposta a incidentes [MITRE 2025a].

Os resultados podem ser relacionados a objetivos de segurança associados ao FR 3 *System Integrity*, ao permitir identificar alterações não autorizadas em parâmetros de ativos [International Electrotechnical Commission 2013]. A relação com o FR 7 *Resource Availability* é indireta, uma vez que o monitoramento passivo pode contribuir para identificar eventos que potencialmente afetem a disponibilidade, embora o experimento não tenha avaliado diretamente métricas de disponibilidade.

3. Arquitetura das Plataformas de Monitoramento Passivo

Dado o cenário de sensibilidade dos dispositivos de campo, a inspeção passiva baseada em Deep Packet Inspection (DPI) atua como uma abordagem não intrusiva fundamental [Barbosa and Pras 2010]. Essas plataformas operam segregando completamente as funções de coleta de dados e análise de processos. O tráfego industrial legítimo não sofre interceptação ou modificação; ele é replicado por meio de configurações de espelhamento de portas em switches centrais para sensores de dados dedicados [Claroty 2026].

A partir dos pacotes de dados espelhados, a inspeção por DPI decodifica a semântica interna dos protocolos industriais (como Modbus TCP, S7comm, EtherNet/IP, DNP3, entre outros). Esse processo viabiliza tanto a construção automatizada do inventário de ativos (fabricante, modelo, versão de firmware) quanto a detecção de incidentes cibernéticos por duas vertentes complementares [Goldenberg and Wool 2013]. A identificação de incidentes ocorre por duas estratégias complementares: detecção por assinaturas, baseada em padrões previamente conhecidos e mapeados no MITRE ATT&CK for ICS, e detecção comportamental, que utiliza um *baseline* da operação normal para identificar anomalias no comportamento dos dispositivos e da comunicação da rede.

4. Experimento Prático

4.1. Ambiente de Laboratório

O experimento foi conduzido em um ambiente controlado de redes industriais, cuja topologia compreende múltiplos ativos de TI e TO, conforme ilustrado na Figura 1. A infraestrutura de testes utilizada envolveu uma estação de engenharia, módulos de aquisição de dados, switches locais de distribuição e um switch industrial central conectado a um

servidor de monitoramento passivo. Um módulo de aquisição de dados foi selecionado como o dispositivo alvo para um cenário de incidente cibernético. A escolha justificou-se pela ampla utilização do dispositivo em aplicações industriais e pela natureza estruturada de seu tráfego periódico, características adequadas para a avaliação de regras de detecção comportamental.

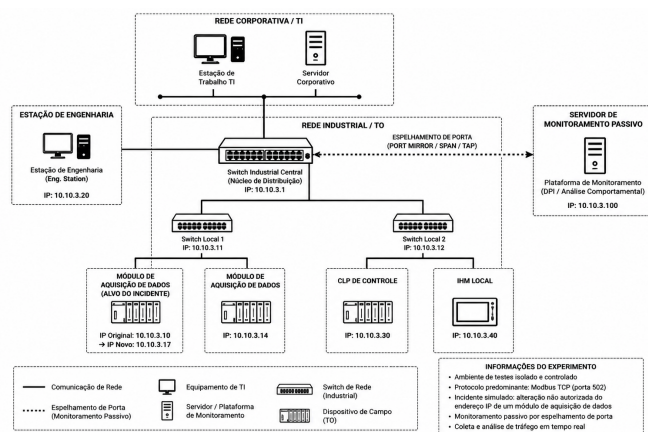


Figura 1. Diagrama de rede do ambiente de laboratório.

4.2. Metodologia de Captura Dual

Para garantir a confiabilidade da análise, implementou-se uma metodologia de captura dual a partir do tráfego replicado pelo switch central. O software Wireshark foi configurado como a ferramenta de inspeção em baixo nível (análise bruta de pacotes), enquanto uma plataforma de monitoramento industrial comercial realizou a interpretação semântica e comportamental dos fluxos de dados em tempo real.

4.3. Cenário de Teste e Resultados

O cenário simulado consistiu na reconfiguração não autorizada de parâmetros de rede de um módulo de aquisição de dados a partir de uma estação de engenharia. O objetivo do incidente simulado foi alterar o endereço IP original do dispositivo (10.10.3.10) para um novo endereço (10.10.3.17). Na plataforma de monitoramento, foi estabelecida uma regra de alerta personalizado para identificar desvios de conduta na rede operacional. Como consequência da alteração, a plataforma disparou um alerta identificado como “Alerta 232” conforme mostra a Figura 2, associado originalmente ao IP 10.10.3.10, registrando o desvio comportamental com precisão cronológica.

☐	ALERT ID	ALERT CATEGORY	ALERT TYPE	DEVICE NAME	DEVICE-ALERT CREATED	DEVICE-ALERT UPDATED
☒	#232	Custom Alert	Custom Communication Alert	10.10.3.10	30/04/2026 11:24	06/05/2026 19:31

Figura 2. Configuração do alerta personalizado na plataforma.

A investigação detalhada do incidente revelou o estabelecimento de uma comunicação bidirecional em Modbus contendo uma inconsistência na rede conforme

apresentado na Figura 3. A estação de engenharia, identificada pelo endereço IP 10.10.3.20, realizou a comunicação com o dispositivo de campo, que passou a responder pelo endereço lógico não autorizado 10.10.3.17, mantendo sua identidade física inalterada.

EVENT ID	FIRST COMM.	LAST COMM.	DESCRIPTION	SIDE A DEVICE ID	SIDE A DEVICE NAME	SIDE A IP	SIDE A DEVICE TYP
#3324	06/05/2026 19:31	06/05/2026 19:31	Internal bidirectional communication over Modbus was detected between 10.10.3.17 (OT Device) and 10.10.3.20 (Engineering Station)	DDHLOAA	10.10.3.10	10.10.3.17	OT Device

Figura 3. Alerta gerado após a alteração de IP do módulo de dados.

O protocolo Modbus TCP não possui uma função ou código de comando dedicado para alterar o endereço IP de um dispositivo. O Modbus TCP apenas encapsula as mensagens de controle (*Read/Write Registers*) dentro de pacotes TCP/IP usando por padrão a porta 502. No entanto, a alteração do endereço IP em dispositivos industriais, dependendo do fabricante e do modelo do dispositivo, pode ocorrer por meio de mecanismos proprietários de gerenciamento e configuração. [Huitsing et al. 2008]. A sequência de ações ocorre da seguinte forma: O dispositivo de configuração envia uma mensagem de *Broadcast* na rede via pacotes UDP em portas de gerência específicas do fabricante; o dispositivo alvo reconhece a mensagem pelo seu Endereço MAC; o configurador envia a requisição de escrita do novo endereço IP para aquele MAC; o dispositivo reconhece o novo IP e reinicia seu serviço de rede. Esta sequência pode ser verificada na Figura 4.

A validação forense em baixo nível foi realizada por meio das capturas do Wireshark. Na estação de engenharia (IP 10.10.3.20), o evento foi registrado entre os quadros (frames) 869 e 890 conforme evidencia a figura, demonstrando as tentativas iniciais de tráfego UDP na porta de gerência/configuração do fabricante e o subsequente fluxo direcionado ao novo endereço IP 10.10.3.17. A consistência entre ambas as capturas corroborou a alteração do parâmetro lógico do dispositivo.

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
868	2026-05-06 19:30:16,796336	10.10.3.20	10.10.3.10	TCP	54	✓	58771 → 582 [ACK] Seq=1 Ack=1 Win=64240 Len=0
861	2026-05-06 19:30:16,857551	10.10.3.20	10.10.3.10	Modbus.	83	✓	Query: Trans: 0; Unit: 1, Func: 16: Write Multiple Registers
862	2026-05-06 19:30:16,956979	10.10.3.10	10.10.3.20	Modbus.	66	✓	Response: Trans: 0; Unit: 1, Func: 16: Write Multiple Registers
863	2026-05-06 19:30:16,973837	10.10.3.20	10.10.3.10	Modbus.	66	✓	Query: Trans: 255; Unit: 1, Func: 3: Read Holding Registers
864	2026-05-06 19:30:16,975668	10.10.3.10	10.10.3.20	Modbus.	315	✓	Response: Trans: 255; Unit: 1, Func: 3: Read Holding Registers
865	2026-05-06 19:30:16,988980	10.10.3.20	10.10.3.10	TCP	54	✓	58771 → 582 [FIN, ACK] Seq=42 Ack=274 Win=63967 Len=0
866	2026-05-06 19:30:16,989385	10.10.3.10	10.10.3.20	TCP	68	✓	582 → 58771 [FIN, ACK] Seq=274 Ack=43 Win=256 Len=0
867	2026-05-06 19:30:16,989432	10.10.3.20	10.10.3.10	TCP	54	✓	58771 → 582 [ACK] Seq=43 Ack=275 Win=63967 Len=0
868	2026-05-06 19:30:16,999352	10.10.3.20	255.255.255.255	UDP	126	✓	68822 → 5848 Len=84
869	2026-05-06 19:30:16,995113	10.10.3.10	10.10.3.20	UDP	182	✓	5848 → 68823 Len=60
870	2026-05-06 19:30:16,928240	10.10.3.20	255.255.255.255	UDP	182	✓	68823 → 5848 Len=60
871	2026-05-06 19:30:16,928976	10.10.3.10	10.10.3.20	UDP	182	✓	5848 → 68823 Len=60
890	2026-05-06 19:30:29,098426	10.10.3.20	10.10.3.17	UDP	47	✓	68824 → 1825 Len=5
891	2026-05-06 19:30:29,095201	10.10.3.17	10.10.3.20	UDP	68	✓	1825 → 68824 Len=8
892	2026-05-06 19:30:29,714865	10.10.3.20	10.10.3.17	UDP	47	✓	68824 → 1825 Len=5
893	2026-05-06 19:30:29,714885	10.10.3.17	10.10.3.20	UDP	68	✓	1825 → 68824 Len=8
894	2026-05-06 19:30:29,715053	10.10.3.20	10.10.3.17	UDP	47	✓	68824 → 1825 Len=5
895	2026-05-06 19:30:29,715088	10.10.3.17	10.10.3.20	UDP	68	✓	1825 → 68824 Len=8

Figura 4. Evento registrado na estação de engenharia.

O sensor passivo registrou o mesmo comportamento no quadro 2292 conforme apresentado na Figura 5, consolidando a troca definitiva de parâmetros lógicos e validando a consistência analítica entre todas as fontes de observação utilizadas no experimento. No cenário avaliado, a sequência observada nas capturas indicou o uso de mensagens UDP/*Broadcast* associadas ao mecanismo de configuração do dispositivo, corroborando a interpretação dos eventos observados.

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
1972	2026-05-06 19:30:21,798903594	10.10.3.20	255.255.255.255	UDP	126	✓	60022 → 5048 Len=84
1973	2026-05-06 19:30:21,798946912	10.10.3.20	255.255.255.255	UDP	126	✓	60022 → 5048 Len=84
1974	2026-05-06 19:30:21,794557329	10.10.3.18	10.10.3.20	UDP	102	✓	5048 → 60022 Len=60
1975	2026-05-06 19:30:21,811787524	10.10.3.20	255.255.255.255	UDP	102	✓	60023 → 5048 Len=60
1976	2026-05-06 19:30:21,811798472	10.10.3.20	255.255.255.255	UDP	102	✓	60023 → 5048 Len=60
1977	2026-05-06 19:30:21,812419051	10.10.3.10	10.10.3.20	UDP	102	✓	5048 → 60023 Len=60
2292	2026-05-06 19:30:34,565078843	10.10.3.20	10.10.3.17	UDP	60	✓	60024 → 1025 Len=5
2294	2026-05-06 19:30:34,582783398	10.10.3.17	10.10.3.20	UDP	60	✓	1025 → 60024 Len=8
2296	2026-05-06 19:30:34,605743027	10.10.3.20	10.10.3.17	UDP	60	✓	60024 → 1025 Len=5
2297	2026-05-06 19:30:34,606492355	10.10.3.17	10.10.3.20	UDP	60	✓	1025 → 60024 Len=10
2298	2026-05-06 19:30:34,622737273	10.10.3.20	10.10.3.17	UDP	60	✓	60024 → 1025 Len=5
2299	2026-05-06 19:30:34,623449361	10.10.3.17	10.10.3.20	UDP	60	✓	1025 → 60024 Len=10
2300	2026-05-06 19:30:34,636833976	10.10.3.20	10.10.3.17	UDP	60	✓	60024 → 1025 Len=5
2301	2026-05-06 19:30:34,637486093	10.10.3.17	10.10.3.20	UDP	60	✓	1025 → 60024 Len=8
2435	2026-05-06 19:30:41,131958034	10.10.3.20	10.10.3.17	TCP	66	✓	58772 → 582 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2436	2026-05-06 19:30:41,132414436	10.10.3.17	10.10.3.20	TCP	60	✓	582 → 58772 [SYN, ACK] Seq=0 Ack=1 Win=256 Len=0 MSS=1460
2437	2026-05-06 19:30:41,133339093	10.10.3.20	10.10.3.17	TCP	60	✓	58772 → 582 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2438	2026-05-06 19:30:41,187418056	10.10.3.20	10.10.3.17	Modbus	83	✓	Query: Trans: 0: Unit: 1: Func: 16: Write Multiple Registers

Figura 5. Evento registrado no sensor passivo.

4.4. Mapeamento ao MITRE ATT&CK for ICS e Ajuste Técnico de Protocolo

Embora o módulo utilize o protocolo Modbus TCP para a comunicação operacional, a alteração do endereço IP não é realizada por esse protocolo. Em dispositivos industriais legados, essa configuração pode ocorrer por meio de mecanismos proprietários de gerenciamento, específicos de cada fabricante, responsáveis pela reconfiguração dos parâmetros de rede.

Sob a ótica do MITRE ATT&CK for ICS, o evento observado corresponde à técnica T0836 – Modify Parameter, vinculada à tática *Impair Process Control* [MITRE 2025b]. Em sistemas SCADA dependentes do endereço IP original do dispositivo, uma alteração não autorizada desse parâmetro pode interromper a comunicação com o ativo e reduzir a visibilidade operacional.

5. Conclusão

A principal contribuição experimental consistiu na correlação entre diferentes níveis de observação: a análise semântica e comportamental realizada pela plataforma de monitoramento e a análise de baixo nível dos pacotes capturados pelo Wireshark. A metodologia de captura dual permitiu correlacionar o alerta comportamental com evidências diretamente observáveis no tráfego de rede, incluindo a associação entre o novo endereço IP e o endereço MAC físico do dispositivo. A análise também evidenciou a importância de distinguir o tráfego operacional Modbus TCP do tráfego de gerenciamento utilizado para a reconfiguração do endereço IP.

Os resultados demonstram que o monitoramento passivo amplia a visibilidade dos ambientes industriais sem interferir no tráfego operacional. A correlação entre a plataforma de monitoramento, as capturas do Wireshark, o MITRE ATT&CK for ICS e os objetivos de segurança da IEC 62443 evidencia o potencial da abordagem para apoiar processos de detecção e investigação de incidentes.

Embora o estudo tenha sido conduzido em ambiente controlado e avaliado um cenário específico, os resultados indicam que o monitoramento passivo constitui um mecanismo relevante para apoiar a visibilidade e a detecção de eventos de segurança, contribuindo indiretamente para objetivos de integridade, disponibilidade e resiliência cibernética de ambientes industriais. Estudos futuros poderão avaliar diferentes cenários com métricas de desempenho e respostas a incidentes.

Agradecimentos

Este trabalho contou com o apoio das empresas CLAVIS Segurança da Informação e CLAROTY por meio do projeto "Segurança cibernética em sistemas de tecnologia operacional (*Cyber OT*) e infraestruturas críticas".

Referências

- Barbosa, R. R. R. and Pras, A. (2010). Intrusion detection in industrial control systems.
- Claroty (2026). Passive monitoring: Collection method overview.
- Goldenberg, N. and Wool, A. (2013). Accurate modeling of modbus/tcp for intrusion detection in scada systems.
- Huitsing, P., Chandia, R., Papa, M., and Shenoi, S. (2008). Attack taxonomies for the modbus protocols.
- International Electrotechnical Commission (2013). Industrial communication networks – network and system security – part 3-3: System security requirements and security levels. Technical report, International Electrotechnical Commission, Geneva, Switzerland.
- Knapp, E. D. and Langill, J. T. (2014). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress.
- MITRE (2025a). Mitre att&ck for ics.
- MITRE (2025b). Modify parameter (t0836) – mitre att&ck for ics.
- National Institute of Standards and Technology (2023). Guide to operational technology (ot) security. Technical report, National Institute of Standards and Technology.
- Williams, T. J. (1994). The purdue enterprise reference architecture. *Computers in Industry*, 24(2–3):141–158.