Um *cyber range* baseado em contêineres para ensino de cibersegurança em tecnologias operacionais e sistemas de controle industrial

Luiz F. Freitas-Gutierres[1,2], Jhonatan A. Cassol[2], Adriano P. Morais[2,3], José J. B. S. Pinto[4], Miguel G. Rodrigues[4], Rafael R. Farias[4], Marisa S. Maximiano[5], Ricardo J. P. Gomes[4]

[1]Departamento de Eletromecânica e Sistemas de Potência
Universidade Federal de Santa Maria (UFSM) – Santa Maria, RS, Brasil

[2]Centro de Excelência em Energia e Sistemas de Potência
Laboratório de Análise e Proteção de Sistemas Elétricos
Universidade Federal de Santa Maria (UFSM) – Santa Maria, RS, Brasil

[3]Colégio Técnico Industrial de Santa Maria
Universidade Federal de Santa Maria (UFSM) – Santa Maria, RS, Brasil

[4]Instituto Politécnico de Leiria (IPLeiria) – Leiria, Portugal

[5]Computer Science and Communication Research Centre (CIIC)
Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Leiria (IPLeiria) – Leiria, Portugal

luiz.gutierres@ufsm.br, adriano@ctism.ufsm.br,

marisa.maximiano@ipleiria.pt, ricardo.p.gomes@ipleiria.pt

Abstract. *This paper introduces OTLabs, emulated operational technology (OT) and industrial control system (ICS) environments designed to support hands-on industrial cybersecurity training in container-based cyber ranges. The approach addresses the need to strengthen practical OT-ICS skills in the face of increasing complexity, ongoing digitalization, and expanding attack surfaces in cyber-physical systems, particularly in the electric and industrial manufacturing sectors. The paper discusses the typical OTLab architecture, the use of orchestration scripts, and the development methodology, covering both technical and educational aspects. In total, thirteen OTLabs were developed, ranging from introductory OT-ICS asset discovery labs to more advanced scenarios. OTLabs have been integrated into undergraduate courses and training programs, with high student acceptance and engagement.*

Resumo. *Este trabalho apresenta os OTLabs, ambientes de emulação de tecnologias operacionais (do Inglês, 'operational technology' [OT]) e sistemas de controle industrial ('industrial control systems' [ICS]), projetados para apoiar a aprendizagem experimental em cibersegurança industrial por meio de 'cyber ranges' baseados em contêineres. A proposta responde à necessidade de fortalecer a formação prática em OT-ICS, diante da crescente complexidade, digitalização e ampliação da superfície de ataque de sistemas ciberfísicos, especialmente nos setores elétrico e de manufatura industrial. São discutidos a arquitetura típica*

dos OTLabs, o uso de 'scripts' de orquestração e a metodologia de desenvolvimento, considerando aspectos técnicos e educacionais. Como resultado, foram desenvolvidos treze OTLabs, que vão de atividades introdutórias de descoberta de ativos OT-ICS a cenários mais complexos. Os OTLabs têm sido aplicados em disciplina de graduação e em treinamentos, com elevada receptividade e engajamento dos discentes.

1. Introdução

Observa-se um crescimento das ameaças cibernéticas direcionadas a infraestruturas críticas, incluindo estações de tratamento de água e esgoto, órgãos governamentais e o setor elétrico [The White House 2013, Stoddart 2022]. No segmento de geração, transmissão e distribuição de energia elétrica, registram-se 63 incidentes catalogados no *cyber incident tracker for electric systems* (CITEPS) até o início do primeiro semestre de 2026, dos quais 13 são classificados como críticos [Freitas-Gutierres 2025]. Adicionalmente, verifica-se um aumento de incidentes com consequências físicas [Waterfall Security Solutions 2024, Waterfall Security Solutions 2025], direcionados a tecnologias operacionais (do Inglês, *operational technology* [OT]) e a sistemas de controle industrial (*industrial control systems* [ICS]), bem como eventos que, embora originados na rede corporativa (*information technology* [IT]), impactam indiretamente os ambientes industriais.

A insuficiência de medidas de segurança em OT-ICS, que abrangem desde controladores lógicos programáveis (CLPs) em indústrias até relés de proteção em subestações, pode resultar em acessos não autorizados, vazamento de informações sensíveis, ataques de *ransomware*, fraudes, sabotagem e interrupção de processos, com consequências potencialmente desastrosas [Flaus 2019, Ackerman 2021, Brooks and Craig Jr. 2022]. Entre os exemplos notórios nesse contexto, destacam-se os ataques direcionados a agentes de distribuição de energia elétrica na Ucrânia, em 2015, e a uma transmissora em 2016 [Zetter 2016a, Zetter 2016b, Styczynski and Beach-Westmoreland 2019]. Esse último foi conduzido com uso do *malware* modular denominado *Industroyer*, que incorporava módulos compatíveis com protocolos e padrões de comunicação empregados em sistemas de supervisão e aquisição de dados (*supervisory control and data acquisition* [SCADA]) e de automação de subestações, incluindo IEC 60870-5-101 (IEC 101), IEC 60870-5-104 (IEC 104), IEC 61850 e OPC [Zetter 2017].

Ao passo que 54% das organizações afirmam estar entre parcialmente preparadas e inseguras frente a futuras ameaças cibernéticas direcionadas a OT-ICS em 2025, aproximadamente 50% dos profissionais de segurança que atuam nesses ambientes possuem cinco anos ou menos de experiência prática [Christopher 2025]. Além disso, 48,7% desses profissionais não possuem certificações em cibersegurança [Christopher 2025], o que pode comprometer a efetividade das medidas de proteção implementadas. No âmbito da educação em Engenharia, nota-se uma carência de linhas formativas voltadas ao desenvolvimento de competências básicas para o trabalho com sistemas ciberfísicos (*cyber-physical systems* [CPS], em Inglês), os quais vêm apresentando crescente convergência com IT [Cao et al. 2020, Yohanandhan et al. 2020]. No contexto europeu, a Diretiva SRI 2 (2022/2555) ampliou significativamente o escopo das obrigações de segurança cibernética para operadores de setores críticos, reforçando a necessidade de capacitação prática em OT-ICS [European Parliament and Council of the European Union 2022]. Relatórios da European

Union Agency for Cybersecurity (ENISA) apontam para um crescimento contínuo das ameaças direcionadas a OT-ICS, acompanhado de uma lacuna de profissionais qualificados para atuar nesses ambientes [Organisation for Economic Co-operation and Development 2024, European Union Agency for Cybersecurity 2025]. À luz disso, torna-se cada vez mais necessário o domínio de conhecimentos relacionados a bancos de dados, estratégias de *backup* e recuperação de dados, virtualização, conteinerização, integração de dispositivos com serviços *web* e, por fim, cibersegurança industrial. A combinação desses conhecimentos com competências em automação e proteção de sistemas elétricos possibilita que os futuros engenheiros colaborem de forma efetiva em equipes multidisciplinares, especialmente junto aos setores responsáveis pela segurança de ativos OT-ICS. Tal base formativa também é essencial para que esses profissionais atuem proativamente em crises cibernéticas, assumindo papel relevante na mitigação de impactos operacionais.

Com o objetivo de endereçar a problemática delineada acima, por meio do uso de *cyber ranges* [National Initiative for Cybersecurity Education 2023] como solução para treinamento prático, este artigo apresenta os **OTLabs: ambientes de emulação OT-ICS estruturados em contêineres, projetados para apoiar a aprendizagem experiencial** [Beard 2010] **e o treinamento em cibersegurança industrial**. Desde o início de 2025, os OTLabs vêm sendo utilizados, com boa receptividade por parte dos discentes, na disciplina complementar de graduação (DCG) intitulada "Fundamentos de Redes e Protocolos para OT-ICS" (UFSM00741), ofertada para cursos de graduação em Engenharia do Centro de Tecnologia (CT) da Universidade Federal de Santa Maria (UFSM). Atualmente, o repositório *free and open-source* (FOSS), disponibilizado publicamente em `https://github.com/substationworm/OTLab`, reúne treze estudos de caso voltados a OT-ICS.

Este trabalho está estruturado da seguinte forma. A Seção 2 apresenta uma visão geral dos OTLabs, relacionando-os aos conceitos de *cyber range*, *infrastructure as code* (IaC) [Muli 2018, Morris 2025] e *scenario-based learning* [Bonwell and Eison 1991, Ward 1998, Errington 2011]. A Seção 3 descreve a metodologia de desenvolvimento dos OTLabs, incluindo seus diagramas de arquitetura típicos e detalhando aspectos educacionais. A Seção 4 apresenta dois exemplos de OTLabs. Por fim, são apresentadas a seção de discussão e as conclusões.

2. Visão geral dos OTLabs

A Figura 1 apresenta a visão geral da arquitetura dos OTLabs, estruturada em três camadas: (i) interação com o usuário, (ii) orquestração e (iii) execução. Na camada de interação, o usuário controla e acessa o OTLab por meio de uma interface de linha de comando (do Inglês, *command-line interface* [CLI]) implementada em *shell script*, `OTLabXY.sh`, em que `XY` representa o identificador do estudo de caso. Esse *script* contempla operações de gerenciamento do ciclo de vida do OTLab, incluindo inicialização (`-start`), interrupção (`-stop`), reinicialização (`-restart`), limpeza (`-clean`), acesso ao ambiente (`-run`) e verificação de estado (`-status`). Dessa forma, abstrai-se a complexidade associada à configuração manual de contêineres e redes virtuais, evitando a necessidade de que os discentes dominem previamente essas habilidades técnicas.

A camada de orquestração é responsável pela declaração da infraestrutura do OTLab, sendo implementada por meio do *Docker Compose*, que opera sobre o *Docker Engine*. Nessa camada, são especificados serviços, redes e dependências necessários para

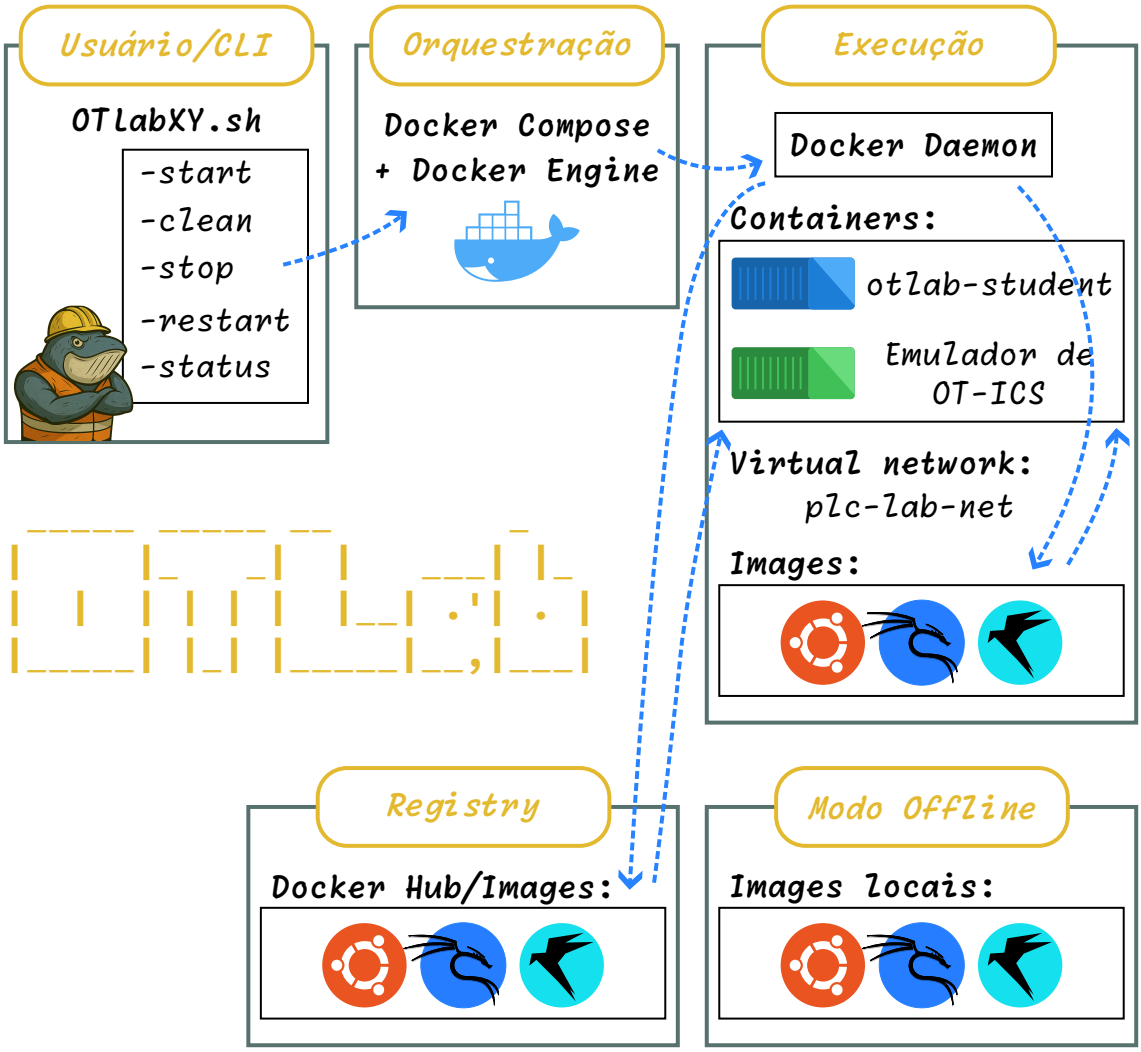

Figura 1. Visão geral da arquitetura dos OTLabs.

a execução de cada cenário, caracterizando uma abordagem alinhada à prática de IaC.

Na camada de execução, o *Docker Daemon* atua como núcleo responsável pela instanciação e pelo gerenciamento dos recursos. O *Daemon* realiza a criação dos contêineres, a configuração da rede virtual dedicada (`plc-lab-net`, na Figura 1) e o gerenciamento das imagens utilizadas. No exemplo apresentado na Figura 1, são instanciados dois contêineres com papéis bem definidos: (i) o contêiner `otlab-student`, que representa o ambiente de interação do discente para análise do problema proposto, e (ii) o contêiner responsável pela emulação de dispositivos OT-ICS. A Figura 2 detalha a organização interna desses contêineres, evidenciando suas funcionalidades. Nos cenários em que é instanciado, o contêiner `otlab-student` agrega, em geral, um conjunto de ferramentas e *scripts* voltados a atividades de reconhecimento, análise e interação com o ambiente emulado, incluindo utilitários de descoberta e varredura de rede, como `netdiscover` e `nmap` [Lyon 2009], bem como ferramentas para captura, inspeção e análise de tráfego, como `tcpdump` e `tshark` [Jain 2022]. Por sua vez, o contêiner de emulação OT-ICS (`otlab-ot-ics`, na Figura 2) incorpora tipicamente ferramentas especializadas para exposição controlada de serviços, como *honeypots* de OT-ICS-SCADA, simuladores de dispositivos e aplicações

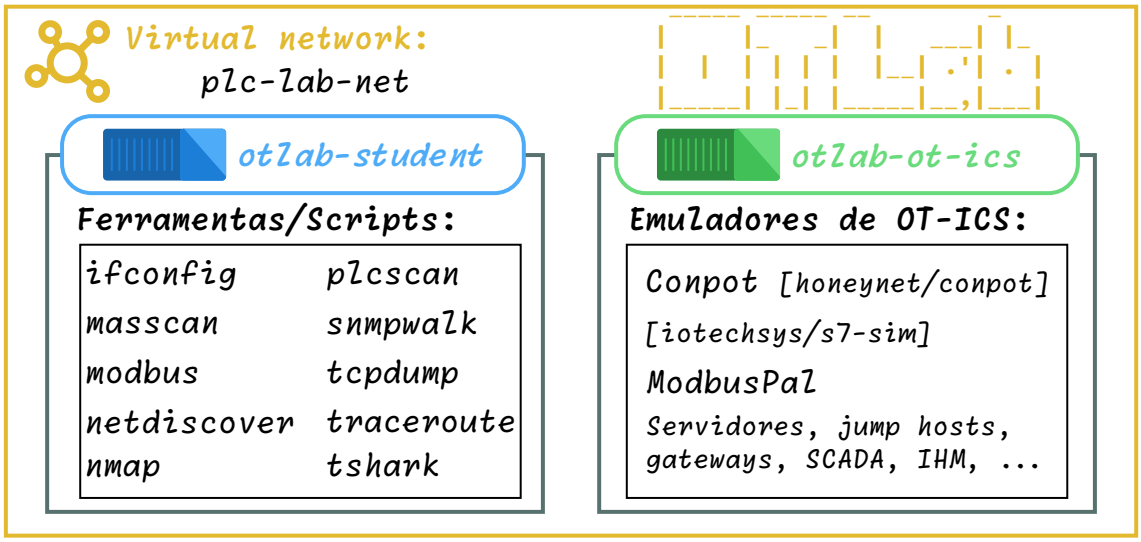

Figura 2. Organização interna típica dos OTLabs.

voltadas a protocolos industriais, como `Conpot`, `s7-sim` e `ModbusPal` [Hopes 2009].

O provisionamento das imagens de contêineres pode ocorrer por dois caminhos distintos. No modo *online*, as imagens são obtidas a partir de um *registry*, como o *Docker Hub*, por meio de operações de *pull*. Alternativamente, no modo *offline*, as imagens são construídas localmente a partir de *Dockerfiles*, permitindo a execução dos OTLabs em ambientes com restrições de conectividade. Ambos os fluxos convergem para o *Docker Daemon*, que é responsável por disponibilizar as imagens para a criação dos contêineres.

3. Metodologia de desenvolvimento dos OTLabs

A metodologia de desenvolvimento dos OTLabs é constituída pelas seguintes etapas: (i) definição de objetivos de ensino-aprendizagem e do cenário de emulação; (ii) modelagem da topologia e seleção de ferramentas e *scripts*; (iii) validação técnica; e (iv) disponibilização no repositório e aplicação em sala de aula ou treinamentos.

Na etapa (i), busca-se adotar como referência o **modelo Purdue (*Purdue enterprise reference architecture* [PERA])** [Ackerman 2021, Stouffer et al. 2023], conforme ilustrado na Figura 3, permitindo a definição dos papéis dos contêineres—abarcando o ambiente de interação do usuário do OTLab e os componentes de emulação de OT-ICS—, assim como a segmentação da rede, os serviços a serem expostos e os protocolos industriais a serem utilizados. O uso de uma arquitetura de referência, conforme a Figura 3, permite também a elaboração de cenários de investigação que contemplam tanto práticas adequadas quanto inadequadas de cibersegurança industrial, incluindo a presença de vulnerabilidades e casos de ataque e resposta a incidentes [Cao et al. 2020].

Os objetivos de ensino-aprendizagem estão orientados principalmente à condução de atividades práticas no âmbito de treinamentos e da disciplina “Fundamentos de Redes e Protocolos para OT-ICS” (UFSM00741), ofertada na UFSM. Nesse sentido, os OTLabs foram desenvolvidos para apoiar o entendimento operacional de ICS, como CLPs, sistemas SCADA, interfaces homem-máquina (IHMs) e unidades remotas terminais (URTs), entre outros. Além disso, os OTLabs visam ao estudo de protocolos de comunicação no domínio

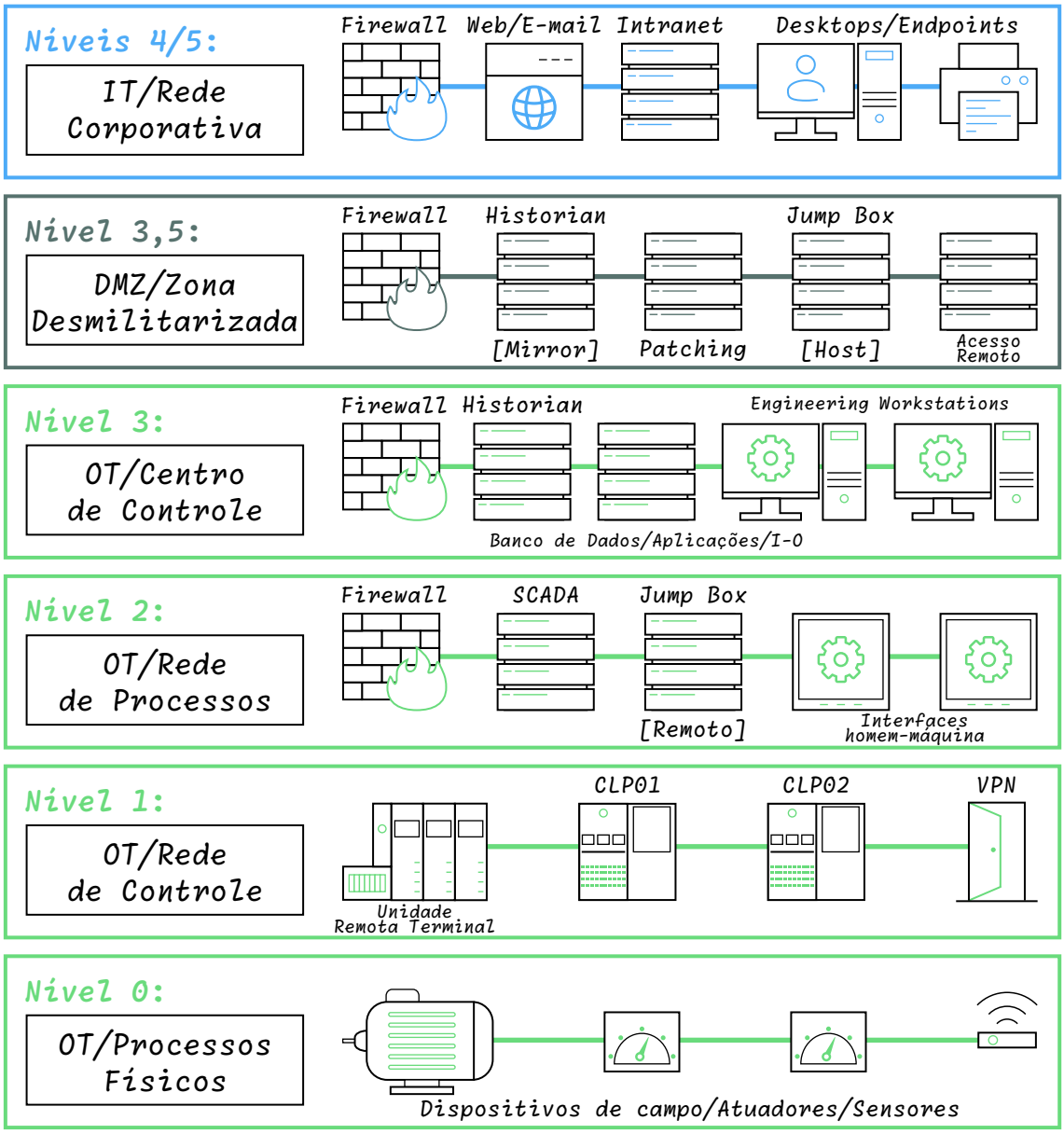

Figura 3. Representação do modelo Purdue.

OT-ICS, abrangendo tanto protocolos comuns de IT, como HTTP, HTTPS e SNMP, quanto protocolos característicos de níveis inferiores do modelo Purdue (níveis 0 e 1) e de sistemas SCADA, como o Modbus [Ackerman 2021, Smith 2021, Brooks and Craig Jr. 2022]. Dentre os objetivos, inclui-se também a análise de topologias de rede industriais, bem como a introdução a fundamentos de cibersegurança industrial.

Na etapa (ii), realiza-se a modelagem da topologia do OTLab e a seleção das ferramentas a serem utilizadas, respeitando uma organização modular dos *scripts* de orquestração. Cada OTLab é estruturado em blocos funcionais bem definidos, a saber:

- **Parametrização global**: Definição de variáveis, como nomes dos contêineres, redes, imagens e demais parâmetros de configuração.
- **Identificação e apresentação**: Rotinas de inicialização, incluindo *banner* de identificação e instruções de uso (*usage*), por meio de funções como `show_banner`.

- **Geração declarativa da infraestrutura**: Construção do arquivo de orquestração com *Docker Compose* (`generate_compose_file`), incluindo:
  - Definição dos contêineres e das ferramentas necessárias.
  - Atribuição de endereços físicos e lógicos (MAC/IP), assim como configuração das redes virtuais.
  - Configuração de comportamentos, serviços e controles de segurança.
- **Verificação de requisitos e funções auxiliares**: Validação de dependências requeridas para execução e definição de funções auxiliares para tratamento de comandos.
- **Gerenciamento do ciclo de vida**: Implementação de uma CLI padronizada para controle do ambiente, com comandos como `-start`, `-run` e `-clean`.

Na etapa (iii) verifica-se a correta execução, a consistência com o comportamento esperado e a reprodutibilidade do OTLab em desenvolvimento. Isso inclui a avaliação da implantação automatizada do ambiente, a realização de testes de conectividade e roteamento entre os diferentes elementos da topologia e a análise dos comportamentos emulados pelos contêineres. Na etapa (iv), os OTLabs são disponibilizados em repositório FOSS, sob licença `CC-BY-4.0`, acompanhados de documentação e tarefas propostas, estando aptos à integração em atividades da disciplina ou em treinamentos.

4. Exemplos de OTLabs

Nesta seção, dois exemplos de OTLabs—**OTLab01** e **OTLab06**—são apresentados em detalhe.

4.1. OTLab01

Em uma única rede virtual, `plc-lab-net`, o OTLab01 é composto por dois contêineres: `otlab-student` e `conpot-plc`. A Figura 4 ilustra as principais características do OTLab01.

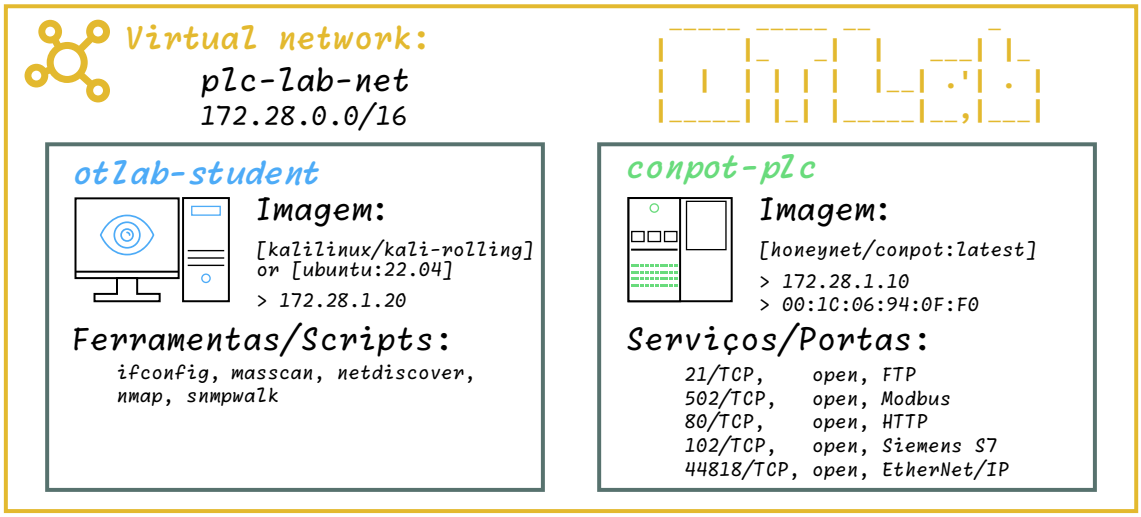

Figura 4. Topologia e características principais do OTLab01.

O contêiner `otlab-student` corresponde ao ambiente de estudo e reconhecimento, com possibilidade de seleção da imagem entre Ubuntu 22.04 e Kali Linux (*rolling*). Nele estão disponíveis ferramentas e *scripts* como `ifconfig`, `masscan`, `netdiscover`,

`nmap` e `snmpwalk`. Por sua vez, o contêiner `conpot-plc` representa o ativo OT-ICS emulado, expondo serviços e portas típicas conforme apresentado na Figura 4, sendo baseado na imagem `honeynet/conpot:latest`, disponibilizada publicamente no *Docker Hub*.

O propósito do OTLab01 é favorecer a execução de atividades introdutórias de descoberta, identificação, coleta de dados e interação com dispositivos industriais emulados, com destaque para protocolos de comunicação como Modbus e Siemens S7. O OTLab01 contempla tarefas de verificação de endereços MAC/IP e de obtenção de informações sobre fabricantes do ativo OT-ICS, sobretudo por meio do uso de ferramentas como `netdiscover` e `nmap`.

De forma complementar, são propostas atividades envolvendo o uso de Google *dorking* [Baker 2023] e de mecanismos de busca especializados, como Shodan [Matherly 2017] e FOFA, para a identificação de ativos OT-ICS publicamente acessíveis que utilizam os mesmos protocolos industriais abordados no estudo de caso. Por fim, o OTLab01 também serve como um treinamento inicial no uso das ferramentas apresentadas na Figura 4, promovendo a familiarização dos discentes com técnicas de reconhecimento em redes industriais e servindo como introdução ao funcionamento geral dos OTLabs.

4.2. OTLab06

O OTLab06, cuja topologia e características principais estão ilustradas na Figura 5, apresenta segmentação em duas redes virtuais, `plc01-net` e `plc02-net`, o que permite avaliar visibilidade parcial e análisar o tráfego entre zonas lógicas. O contêiner `otlab-student` atua como *workstation* para a condução dos estudos e funciona como nó *dual-homed*, conectado a ambas as redes. O OTLab06 combina ativos OT-ICS com quatro funções distintas: um servidor Modubs (`plc01-slave`), um cliente mestre Modbus (`plc02-master`), um *honeypot* servindo como sistema SCADA com interface *web* (`plc03-scada`) e um emulador de Siemens S7 (`plc04-s7`).

Do ponto de vista didático, o OTLab06 contempla duas dimensões de análise em cibersegurança industrial. A primeira refere-se à exposição de uma interface *web* associada a um sistema SCADA, representada pelo contêiner `plc03-scada`. Nesse caso, o ambiente emula um ativo OT-ICS acessível via HTTP, sem mecanismos de autenticação, permitindo a identificação de superfícies de ataque e a discussão de práticas inadequadas de segurança, como a exposição indevida de interfaces de supervisão de processos [Cybersecurity & Infrastructure Security Agency 2025].

A segunda dimensão está relacionada à análise do tráfego gerado entre os contêineres `plc02-master` e `plc01-slave`, no contexto do protocolo Modbus/TCP. O contêiner mestre realiza requisições periódicas ao servidor Modbus, possibilitando a observação e inspeção do tráfego por meio de ferramentas como o `tcpdump`. Como parte das atividades propostas, os discentes são incentivados a identificar padrões de comunicação e a extrair mensagens embutidas no tráfego.

5. Discussão

- Os OTLabs permitem a adoção de uma abordagem gamificada no processo de ensino-aprendizagem [Kapp 2012], podendo ser empregados tanto como atividades práticas ou treinamentos quanto como **instrumentos de avaliação no formato de *capture the flag* (CTF)** [van Rensburg and Baker 2021]. Desde o primeiro

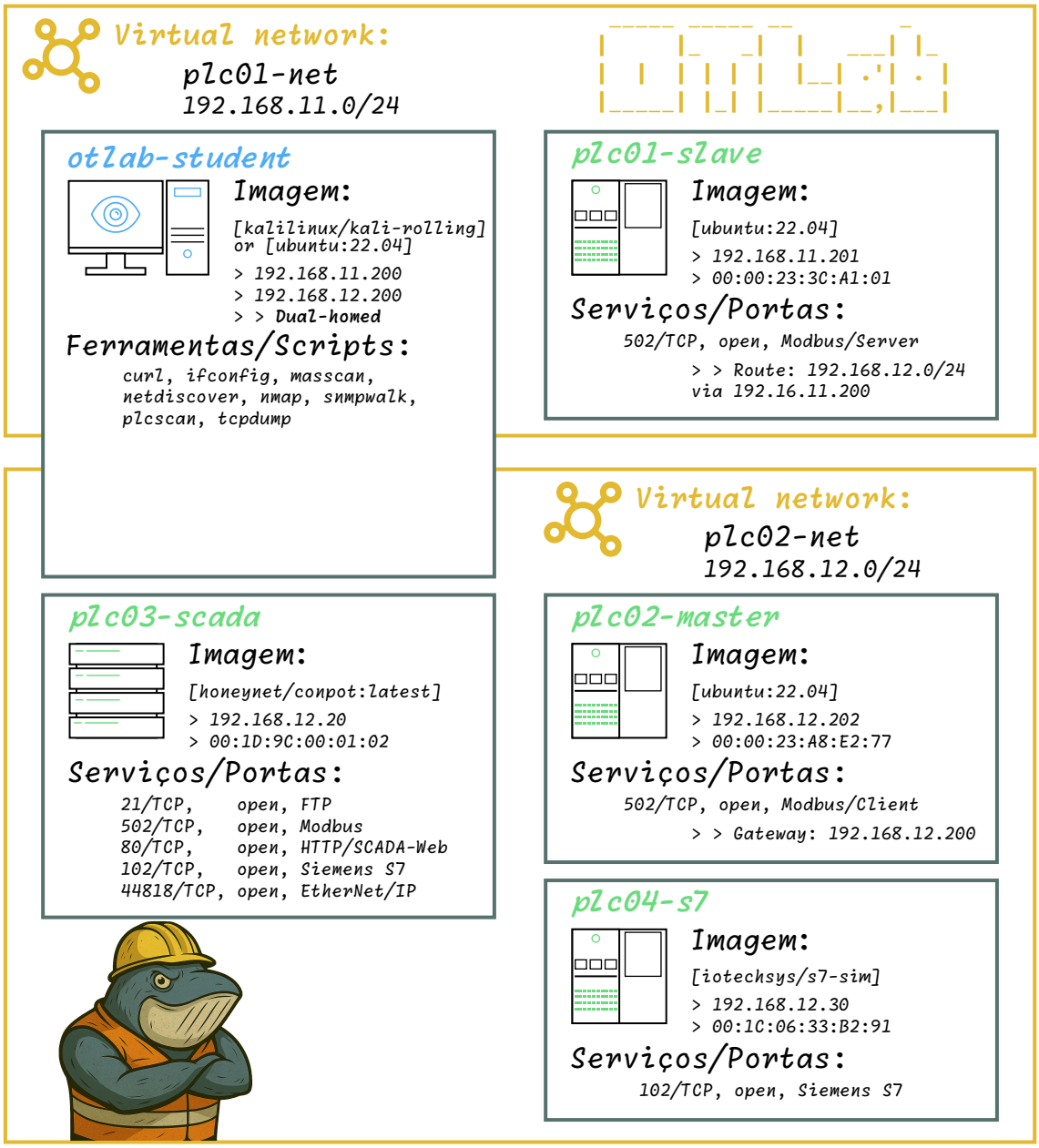

Figura 5. Topologia e características principais do OTLab06.

semestre de 2025, os OTLabs vêm sendo adaptados como CTF e utilizados como a principal estratégia de avaliação da disciplina “Fundamentos de Redes e Protocolos para OT-ICS” (UFSM00741), ofertada na UFSM, com elevado engajamento dos discentes. A combinação de desafios técnicos com narrativas imersivas contribui para a promoção do pensamento crítico, da capacidade de resolução de problemas e do trabalho em grupo, tornando o processo de ensino-aprendizagem mais ativo.

- A disponibilização dos OTLabs em repositório FOSS favorece a colaboração da comunidade, permitindo a melhoria contínua e o desenvolvimento de novos estudos de caso. Tal abordagem é especialmente relevante em OT-ICS e na cibersegurança industrial, reduzindo barreiras de custo e acesso em comparação a *testbeds* físicos de CPS [Yohanandhan et al. 2022a, Yohanandhan et al. 2022b].

- Do ponto de vista operacional, os OTLabs apresentam elevada facilidade de implantação, sendo adequados para uso em laboratórios de informática de universidades, institutos e empresas que possuem restrições de configuração e privilégios de acesso.

6. Conclusões

Este trabalho apresentou os **OTLabs—uma solução de *cyber range* baseada em contêineres para o ensino experimental de cibersegurança industrial**. A proposta foi motivada pela necessidade de ampliar e fortalecer a formação em OT-ICS de engenheiros e profissionais de segurança, especialmente diante da crescente complexidade e exposição de CPS, com ênfase nos setores elétrico e de manufatura industrial. Nesse sentido, foram desenvolvidos treze OTLabs, disponibilizados publicamente em `https://github.com/substationworm/OTLab`. A metodologia de desenvolvimento foi idealizada para torná-los reprodutíveis, modulares e de fácil uso, com comandos simples como `-start`, `-stop` e `-clean`. Como trabalhos futuros, destacam-se a ampliação do conjunto de cenários e de suas complexidades, a incorporação de novos protocolos industriais e casos de uso, bem como a integração com iniciativas de pesquisa, desenvolvimento tecnológico e extensão universitária voltadas à segurança cibernética de infraestruturas críticas.

No âmbito da colaboração entre a Universidade Federal de Santa Maria (UFSM) e o Instituto Politécnico de Leiria (IPLeiria), prevê-se o desenvolvimento de OTLabs com foco em competências de cibersegurança no domínio de IT, complementando os cenários OT-ICS já existentes e consolidando uma abordagem integrada IT-OT. Paralelamente, está prevista a produção de documentação para apoiar a adoção dos OTLabs em contextos educacionais europeus, contribuindo para a disseminação da iniciativa em instituições além do Brasil.

Agradecimentos

Os autores agradecem ao Programa Pesquisador Gaúcho (PqG, Edital 09/2023), da Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS), pelo apoio ao projeto "[PHISHING002] Plataforma de código aberto para avaliação de vulnerabilidades em infraestruturas críticas frente a ataques de *phishing*" (24/2551-0001492-6). As ações vinculadas aos OTLabs contam, ainda, com fomento parcial da Universidade Federal de Santa Maria (UFSM), por meio dos Fundos de Incentivo à Pesquisa (FIPE), à Inovação Tecnológica (FINOVA), ao Ensino (FIEN) e à Extensão (FIEX).

Referências

Ackerman, P. (2021). *Industrial Cybersecurity*. Packt Publishing, Birmingham, UK.

Baker, R. (2023). *Deep Dive: Exploring the Real-World Value of Open Source Intelligence*. John Wiley & Sons, Hoboken, NJ, USA.

Beard, C. (2010). *The Experiential Learning Toolkit: Blending Practice with Concepts*. Kogan Page, New York, NY, USA.

Bonwell, C. C. and Eison, J. A. (1991). *Active Learning: Creating Excitement in the Classroom*. The George Washington University, School of Education and Human Development, Washington, DC, USA.

Brooks, C. B. and Craig Jr., P. A. (2022). *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT*. John Wiley & Sons, Hoboken, NJ, USA.

Cao, L., Jiang, X., Zhao, Y., Wang, S., You, D., and Xu, X. (2020). A Survey of Network Attacks on Cyber-Physical Systems. *IEEE Access*, 8:44219–44227.

Christopher, J. D. (2025). The State of ICS/OT Security 2025. *SANS Institute*. https://bit.ly/4uUOXuz.

Cybersecurity & Infrastructure Security Agency (2025). *Unsophisticated Cyber Actor(s) Targeting Operational Technology*. https://bit.ly/47nHTNc.

Errington, E. (2011). Mission Possible: Using Near-World Scenarios to Prepare Graduates for the Professions. *International Journal of Teaching and Learning in Higher Education*, 23:84–91.

European Parliament and Council of the European Union (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*. NIS2 Directive. https://bit.ly/4m10FQs.

European Union Agency for Cybersecurity (2025). *ENISA Threat Landscape 2025*. https://bit.ly/4uULuw5.

Flaus, J.-M. (2019). *Cybersecurity of Industrial Systems*. John Wiley & Sons–ISTE, Hoboken, NJ, USA.

Freitas-Gutierres, L. F. (2025). *CITEPS: Cyber Incident Tracker for Electric Power Systems*. GitHub [substationworm]. https://github.com/substationworm/CITEPS.

Hopes, J., editor (2009). *Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting*. Syngress Publishing, Burlington, MA, USA.

Jain, V. (2022). *Wireshark Fundamentals: A Network Engineer's Handbook to Analyzing Network Traffic*. Apress, San Jose, CA, USA.

Kapp, K. M. (2012). *The Gamification of Learning and Instrution*. Pfeiffer-ASTD, San Francisco, CA, US.

Lyon, G. (2009). Nmap Network Scanning.

Matherly, J. (2017). *Complete Guide to Shodan*. Leanpub, British Columbia, CA.

Morris, K. (2025). *Infrastructure as Code: Designing and Delivering Dynamic Systems for the Cloud Age*. O'Reilly Media, Sebastopol, CA, USA, 3 edition.

Muli, J. (2018). *Beginning DevOps with Docker*. Packt Publishing, Birmingham, UK.

National Initiative for Cybersecurity Education (2023). The Cyber Range: A Guide. *National Institute of Standards and Technology*. https://bit.ly/4tvnBtN.

Organisation for Economic Co-operation and Development (2024). *Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland*. OECD Skills Studies, OECD Publishing, Paris. https://bit.ly/4seVmys.

Smith, P. (2021). *Pentesting Industrial Control Systems*. Packt Publishing, Birmingham, UK.

Stoddart, K. (2022). *Cyberwarfare: Threats to Critical Infrastructure*. Palgrave Macmillan, Cham, Switzerland.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., and Thompson, M. (2023). Guide to Operational Technology (OT) Security. *National Institute of Standards and Technology*. NIST Special Publication 800-82r3.

Styczynski, J. and Beach-Westmoreland, N. (2019). When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure. *Booz Allen Hamilton*. https://bit.ly/44BF2iS.

The White House (2013). *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*. https://bit.ly/4ipxuTu.

van Rensburg, A. J. and Baker, R. (2021). *CTF Events: Contemporary Practices and State-of-the-Art in Capture-the-Flag Competitions. European Union Agency for Cybersecurity*. https://bit.ly/4sxDAal.

Ward, R. (1998). Active, Collaborative and Case-Based Learning with Computer-Based Case Scenarios. *Computers & Education*, 30:103–110.

Waterfall Security Solutions (2024). *2024 Threat Report*. https://bit.ly/4lu6ZOX.

Waterfall Security Solutions (2025). *2025 Threat Report*. https://bit.ly/40ohpYa.

Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., and Mihet-Popa, L. (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access*, 8:151019–151064.

Yohanandhan, R. V., Elavarasan, R. M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., and Terzija, V. (2022a). A Holistic Review on Cyber-Physical Power System (CPPS) Testbeds for Secure and Sustainable Electric Power Grid – Part – I: Background on CPPS and Necessity of CPPS Testbeds. *International Journal of Electrical Power & Energy Systems*, 136.

Yohanandhan, R. V., Elavarasan, R. M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., and Terzija, V. (2022b). A Holistic Review on Cyber-Physical Power System (CPPS) Testbeds for Secure and Sustainable Electric Power Grid – Part – II: Classification, Overview and Assessment of CPPS Testbeds. *International Journal of Electrical Power & Energy Systems*, 137.

Zetter, K. (2016a). Everything We Know About Ukraine's Power Plant Hack. *WIRED*. https://bit.ly/4irumqn.

Zetter, K. (2016b). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED*. https://bit.ly/3EAwDld.

Zetter, K. (2017). 'Crash Override': The Malware That Took Down a Power Grid. *WIRED*. https://bit.ly/44XLq0y.