CPS Cybersecurity

Do ICS ao CPS:

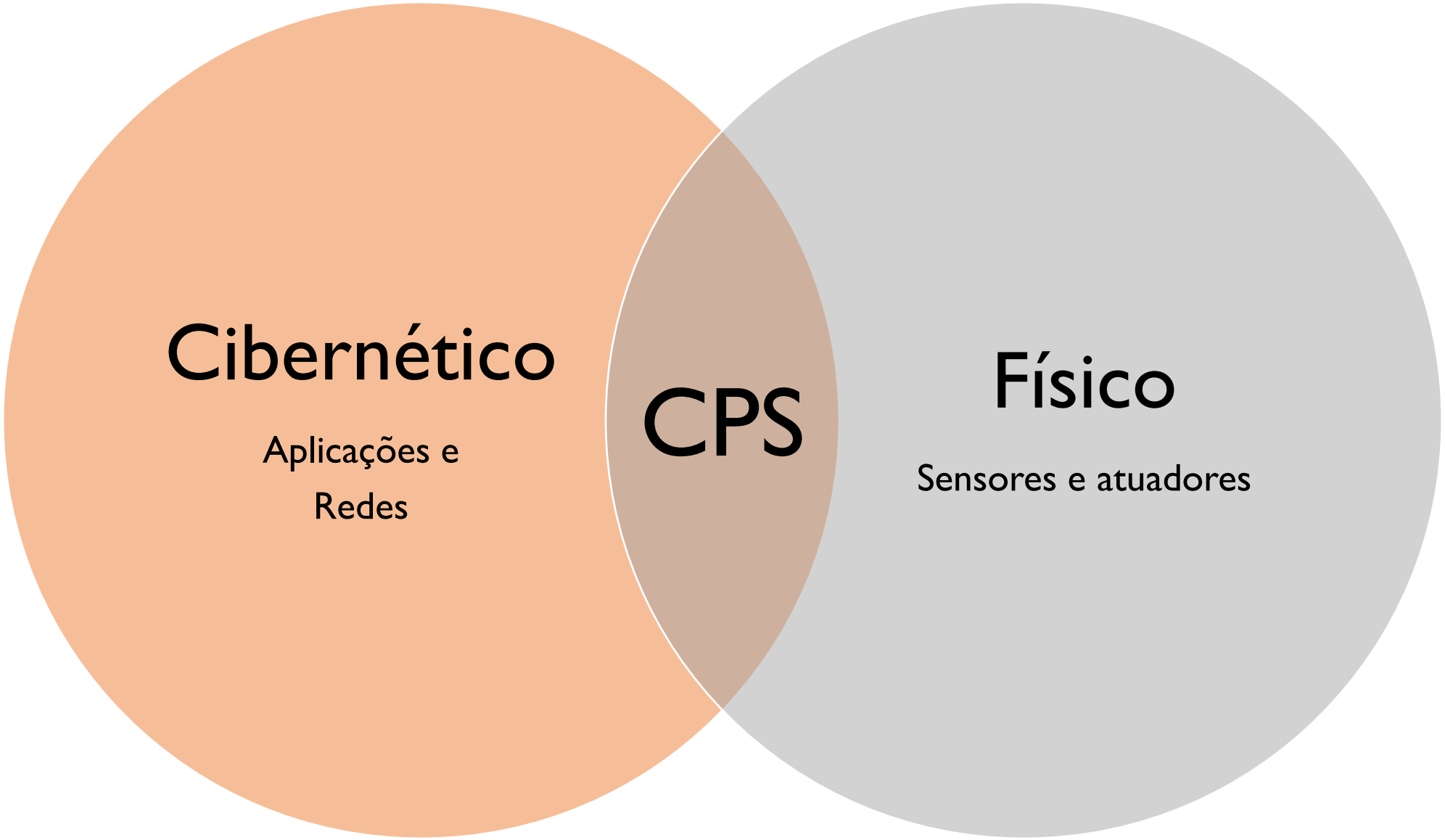
A Nova Era da Cibersegurança em Petróleo e Gás

Marcelo Branquinho | CEO – TI Safe

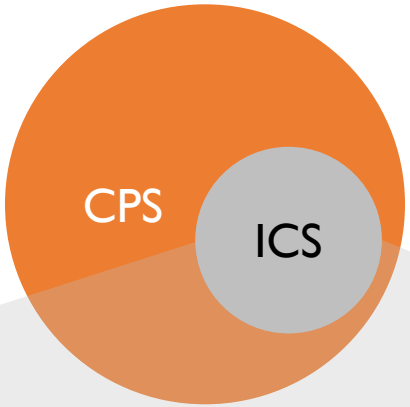
Sobre o apresentador

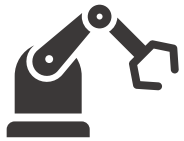
- **Marcelo Ayres Branquinho** é engenheiro eletricista, especialista em segurança cibernética industrial e CEO da TI Safe, empresa pioneira no Brasil dedicada à proteção de infraestruturas críticas. Reconhecido internacionalmente.
- Diretor do CCI para o Brasil, autor de livros técnicos e palestrante em eventos nacionais e internacionais, é membro sênior da ISA Internacional, com atuação nos comitês da norma ISA/IEC-62443.

Sistemas Ciberfísicos (Cyber-Physical Systems – CPS)



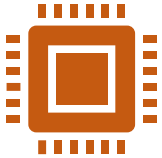
Um sistema de controle industrial (ICS) é um CPS





Aquisição e atuação

- Dispositivos de campo
- Sensores
- Medidores



Conversão

- PLC
- IED
- RTU

Comunicação

- Protocolos
- Equipamentos de rede
- Bancos de dados

Controle

- Supervisório
- HMI

ICS segue uma doutrina (ISA 95)

Nível 4

- Planejamento estratégico e logística

Nível 3

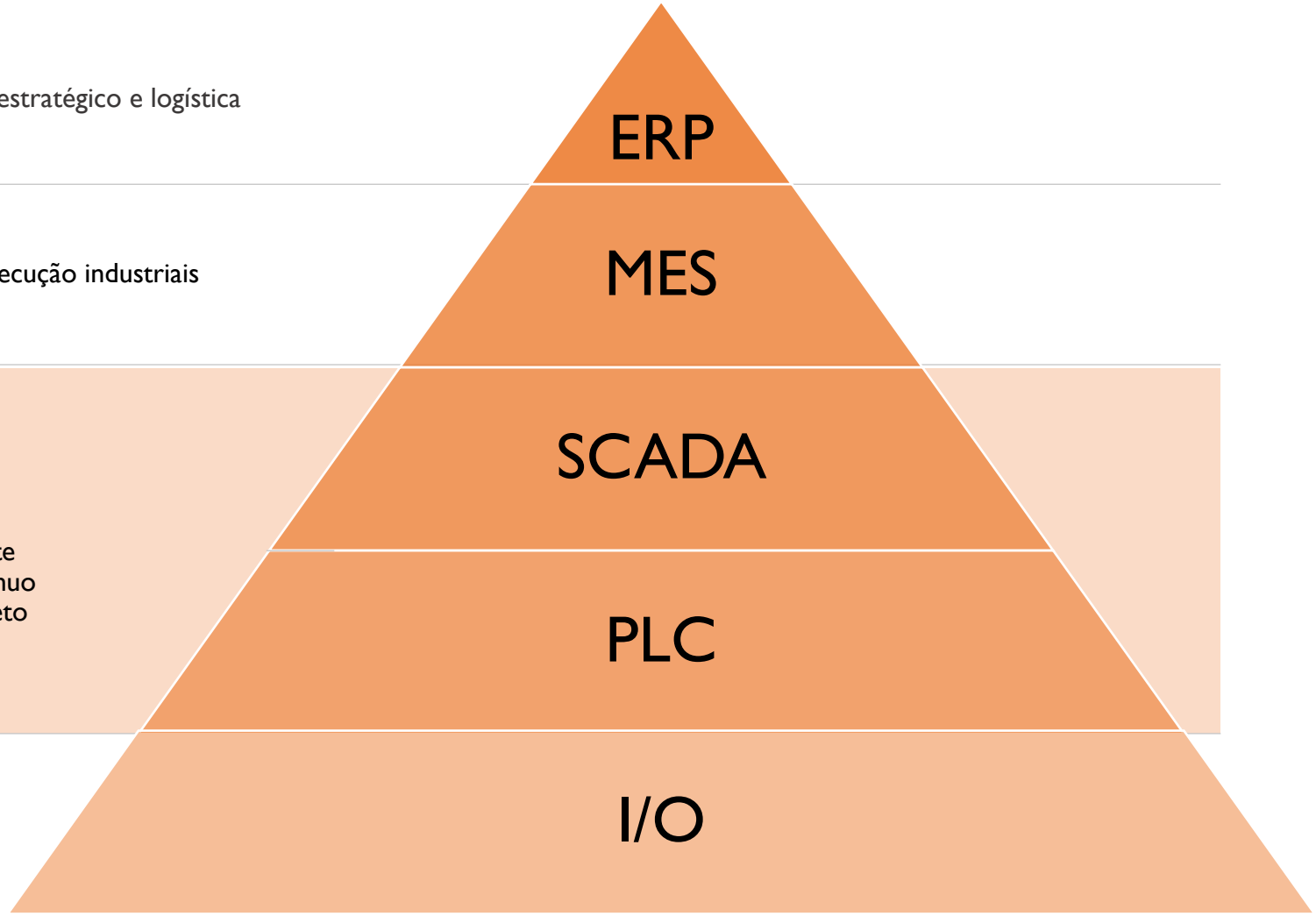
- Sistemas de execução industriais

Níveis 2 e 1

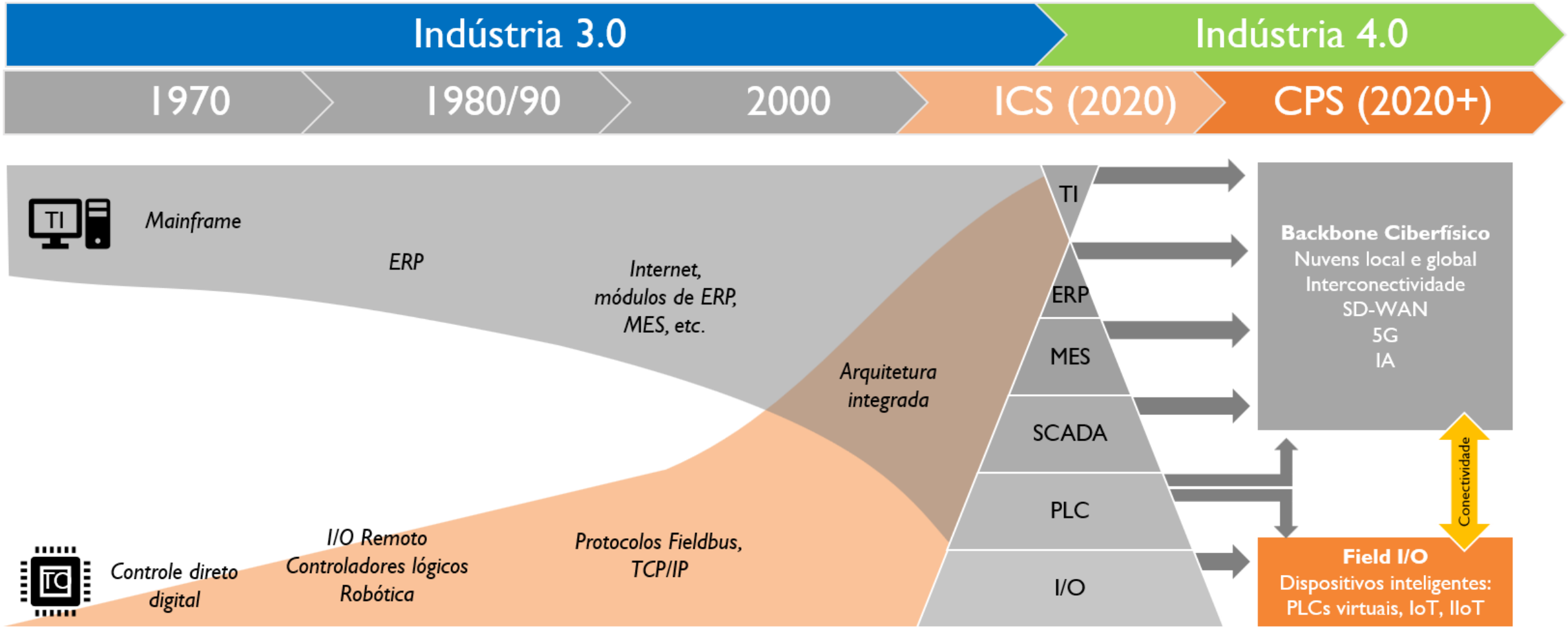
- Controle de lote
- Controle contínuo
- Controle discreto

Nível 0

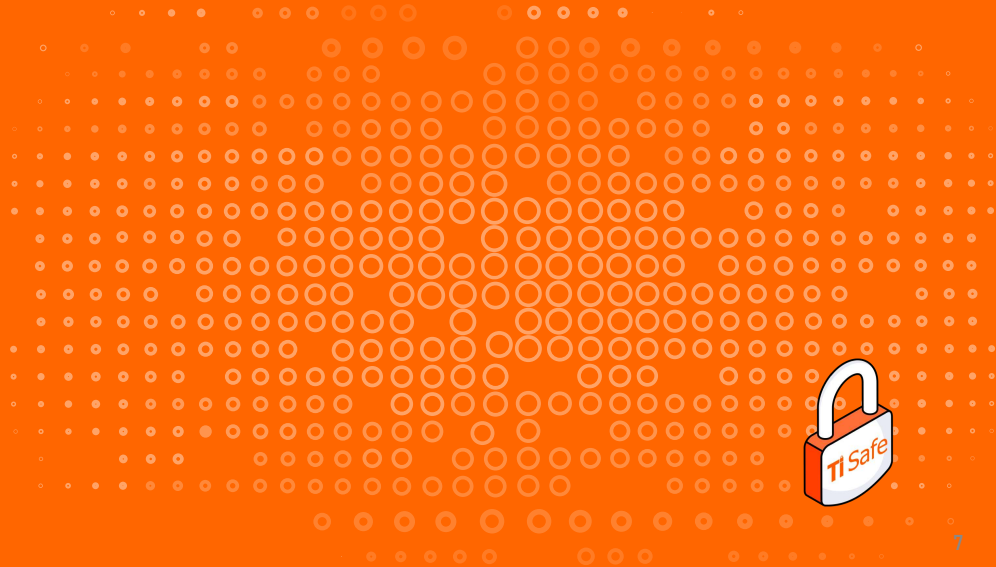
- Sensores e atuadores



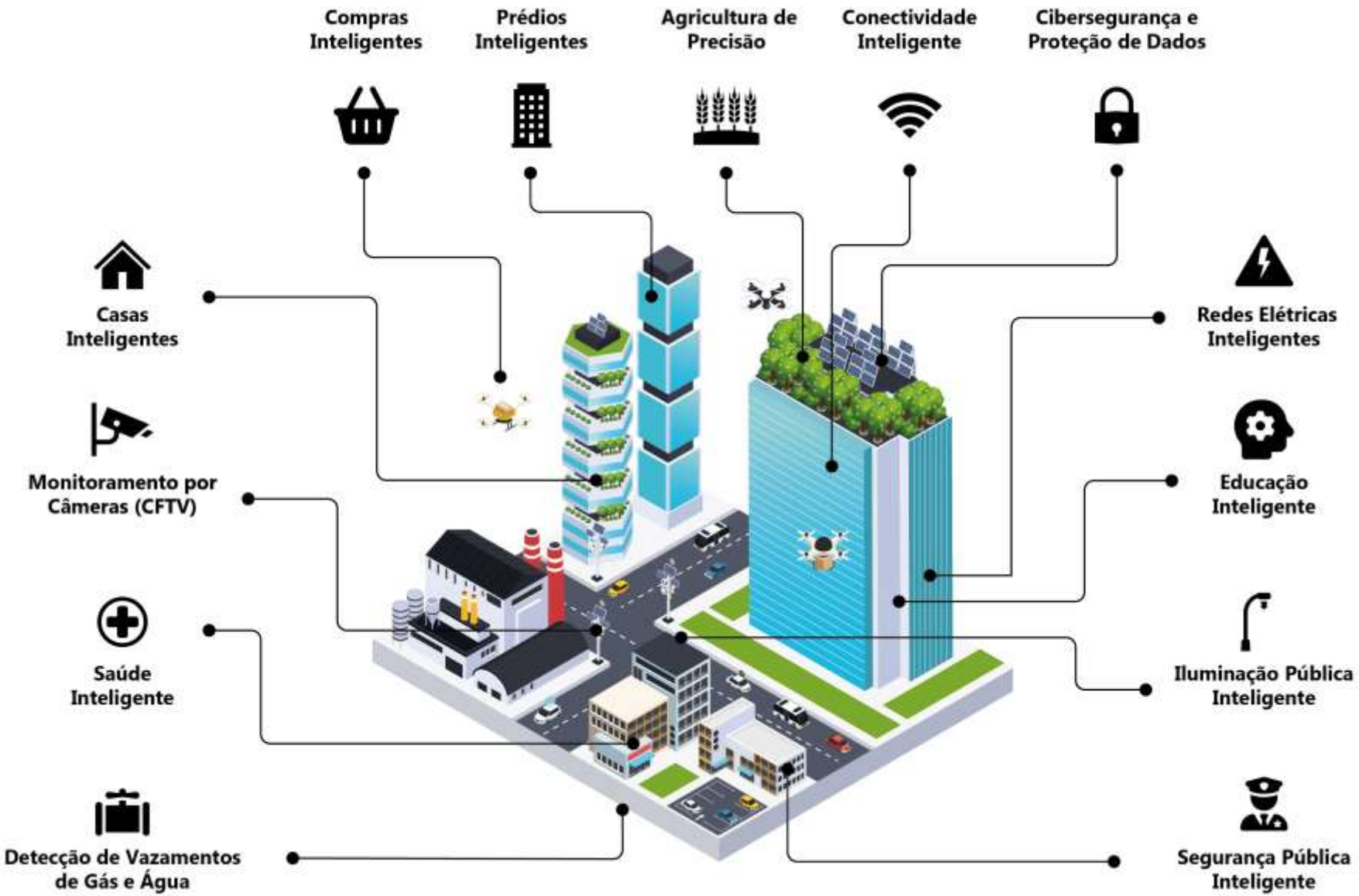
A busca pela eficiência criou os CPS
RIP Modelo Purdue



CPS fazem um mundo *smart*

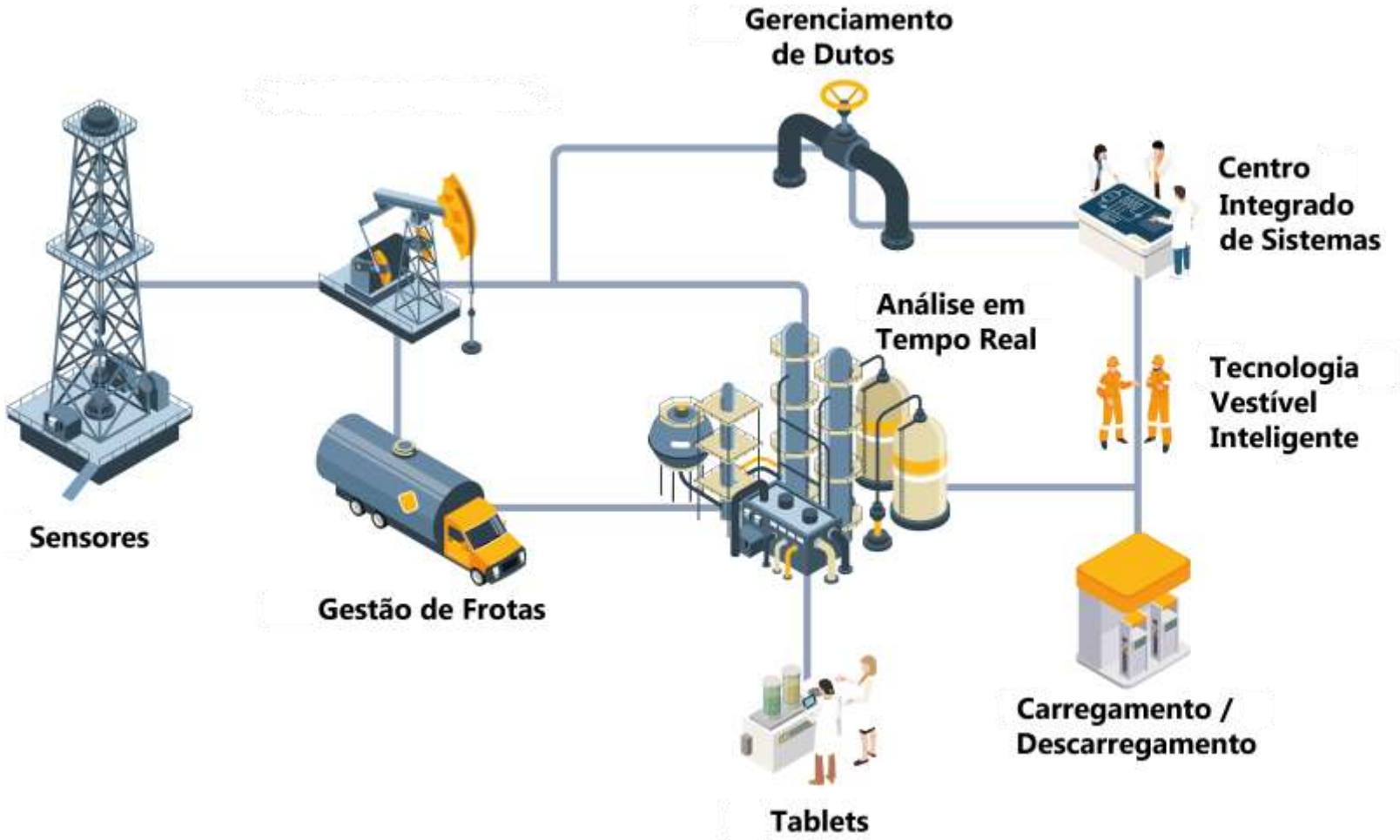


Cidades Inteligentes (Smart Cities)



CPS na indústria de petróleo e gás – Smart Oil & Gas

- Os CPS permitem o monitoramento em tempo real de operações críticas, melhorando a eficiência operacional e possibilitando respostas imediatas a falhas ou desvios.
- Essa tecnologia contribui para a sustentabilidade ambiental, ao facilitar a gestão inteligente de recursos e reduzir desperdícios.
- Em plataformas offshore e refinarias complexas, a coleta e o processamento de informações em tempo real ajudam a prever falhas, otimizar o desempenho e mitigar riscos.
- Redes de gasodutos, que se estendem por milhares de quilômetros, agora utilizam sensores inteligentes e tecnologias IoT para monitorar integridade estrutural, identificar vazamentos e evitar desastres.



IoT na indústria de petróleo e gás – Exemplos de “Things”

1. Atuadores de Válvula Automatizados

- Esses dispositivos são controlados remotamente para abrir e fechar válvulas em sistemas de produção, injeção e segurança, garantindo operações seguras e eficientes. Estão integrados com sistemas DCS (Distributed Control Systems, frequentemente utilizado em FPSOs.

2. Sistema de Monitoramento de Gás (Gas Detectors)

- Esses sensores detectam vazamentos de gases inflamáveis, como metano, e acionam alarmes de emergência. Eles são distribuídos por áreas críticas das plataformas para detecção precoce de riscos à segurança humana e ambiental.

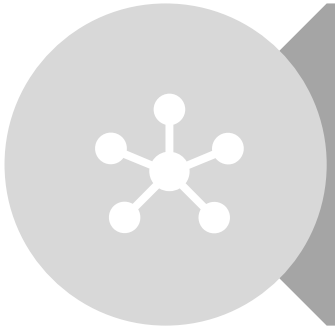
3. Sistemas de Monitoramento de Vibração em Compressores e Bombas

- Utilizados para manutenção preditiva. Esses sensores IoT coletam dados de vibração para detectar desalinhamentos, falhas em rolamentos ou desequilíbrios, permitindo agendamento de manutenção antes que ocorram falhas críticas.

Arquitetura simplificada de CPS

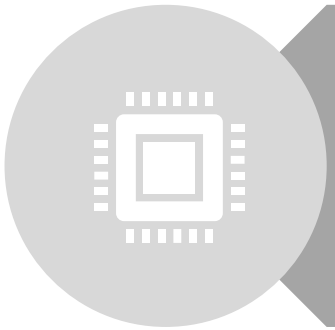
Processamento e controle

- Plataformas de aplicações, armazenamento e processamento de dados em nuvem, que recebem os dados de sensores e enviam comandos aos atuadores



Sistemas de comunicação

- Estruturas de comunicação entre duas ou mais partes das redes inteligentes

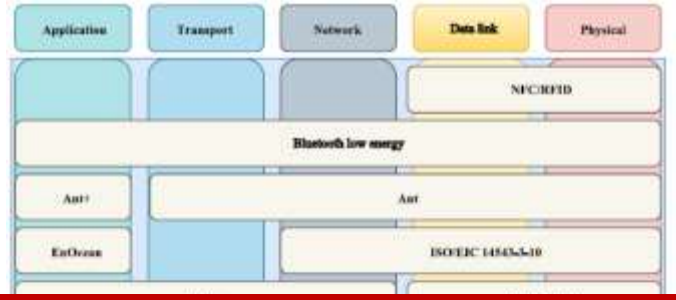


Dispositivos

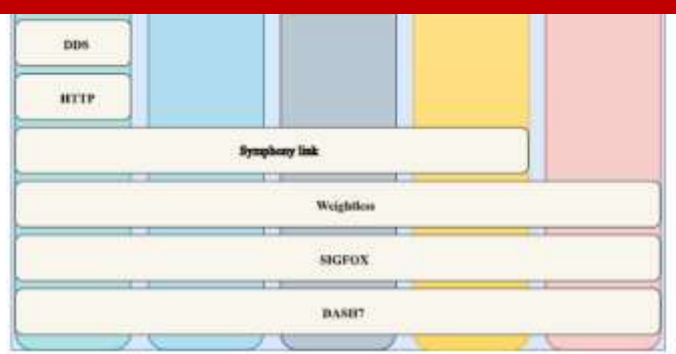
- Dispositivos e sistemas que tocam o mundo físico, como sensores, atuadores, drones, veículos autônomos e telas de smartphones

CPS tornam o mundo frágil

Infinitos dispositivos x Infinitos protocolos x Infinitas aplicações



= Infinitas possibilidades de ataque

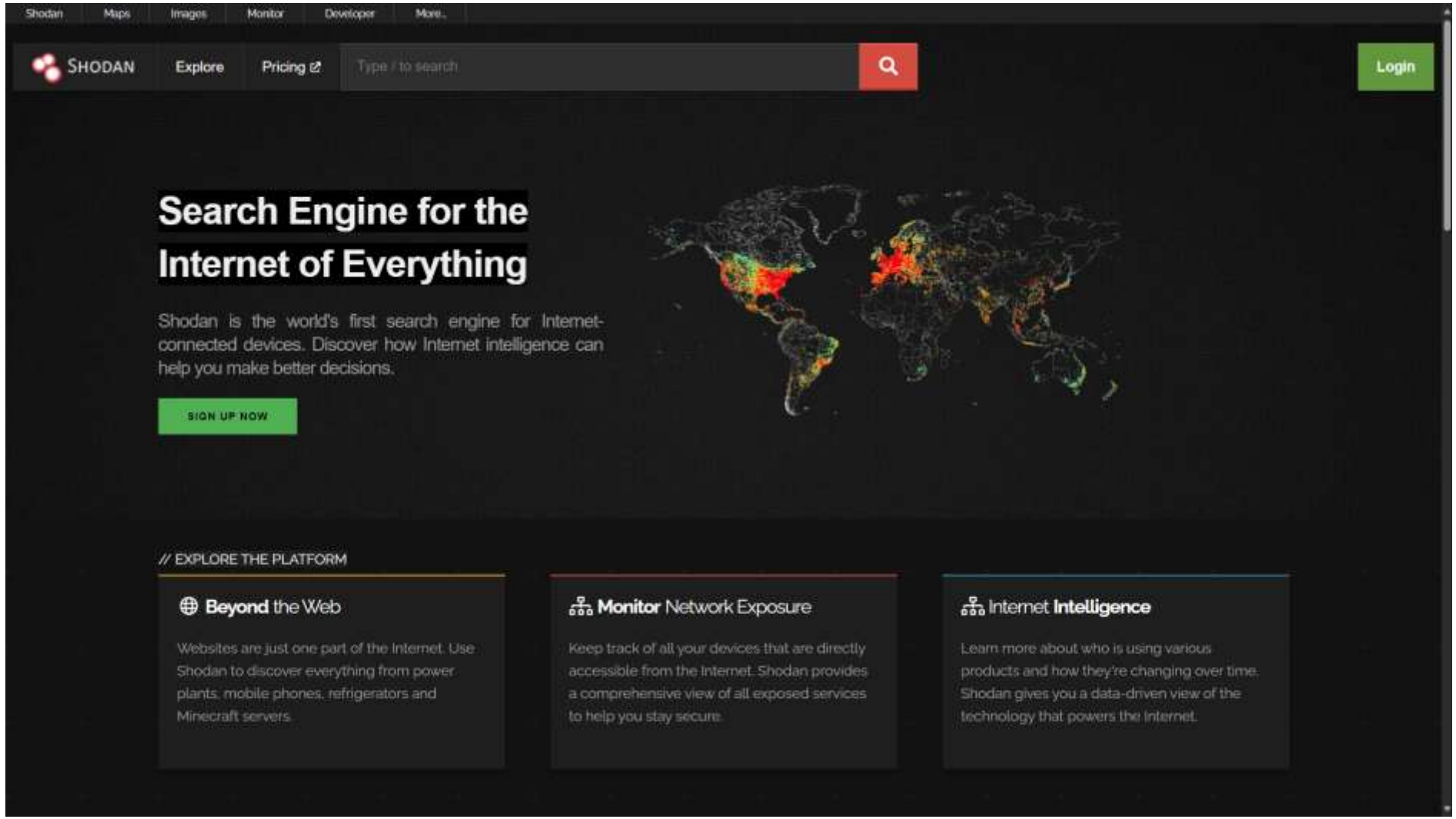


Ameaças gerais aos CPS

	Ameaças cibernéticas
Processamento e controle • Plataformas de aplicações, armazenamento e processamento de dados em nuvem, que recebem os dados de sensores e enviam comandos aos atuadores	Ataques às aplicações
	Ataques a integridade e confidencialidade de dados
Sistemas de comunicação • Estruturas de comunicação entre duas ou mais partes das redes inteligentes	Ataques às redes
	Ataques a integridade e confidencialidade de dados
Dispositivos • Dispositivos e sistemas que tocam o mundo físico, como sensores, atuadores, drones, veículos autônomos e telas de smartphones	Ataques aos dispositivos
	Ataques às interfaces e apps

Infraestruturas de petróleo e gás estão expostas na Web

https://www.shodan.io/



Ataques possíveis e comprovados

- Ataques físicos
  - Violação de dispositivos
  - Injeção de falha
  - Engenharia social
  - Injeção de código
- Ataques de rede
  - MITM
  - DoS
  - Replay
  - Replicação de nó
- Ataques de software
  - Malware
  - 0-Day
  - XSS
  - Alteração de configurações
- Ataques sobre os dados
  - Violação e exposição de dados
  - Ransomware
  - Alteração de dados
  - Destruição de dados
- Ataques por canal lateral
  - Interferência de sinal
  - EMP
- Ataques de privacidade
  - Identificação
  - Rastreamento
  - Extorsão
- Ataques de superfície
  - Sistema operacional
  - Firmware
  - Aplicações

Uma grande quantidade de ataques documentados - Visitem hub.tisafe.com

Os ataques ao OT têm um contexto “conhecido”, como o do Colonial Pipeline (2014)

- Ataque por Ransomware ao Colonial Pipeline, em maio de 2021, nos Estados Unidos. O grupo responsável, identificado como DarkSide, interrompeu digitalmente as operações do maior oleoduto do país, causando escassez de combustível, pânico em diversos estados e impactos econômicos diretos.
- A empresa acabou cedendo à extorsão, pagando cerca de US$ 4,4 milhões em criptomoedas para restaurar o acesso aos sistemas.
- Esse caso demonstrou como o ransomware deixou de ser um problema apenas digital e passou a representar uma ameaça real à infraestrutura crítica e à segurança nacional.

No contexto de CPS, a superfície de ataque é muito maior

- **Atuadores de Válvula Automatizados** — Comprometimento via Protocolo Industrial
  - Risco: Atacantes exploram vulnerabilidades em protocolos industriais (como Modbus/TCP ou FOUNDATION Fieldbus) utilizados em sistemas DCS
  - Impacto: Abertura ou fechamento indevido de válvulas pode causar interrupções no processo, vazamentos ou falhas em sistemas de segurança, como ESD (Emergency Shutdown).
  - Exemplo de ataque: Injeção de comandos falsos via conduítes mal segmentados, comprometendo a integridade do processo e segurança física.
- **Sistemas de Monitoramento de Gás** — Falsificação de Leituras e Inibição de Alarmes
  - Risco: Sensores distribuídos podem ser alvo de spoofing ou DoS (negação de serviço), impedindo a detecção de vazamentos de gases inflamáveis.
  - Impacto: Atraso na resposta a emergências, aumentando o risco de explosões e contaminações.
  - Técnica: Interferência RF (frequência de rádio) ou ataques à integridade de firmware em sensores não autenticados.
- **Sensores de Vibração em Bombas e Compressores** — Sabotagem de Manutenção Preditiva
  - Risco: Acesso não autorizado a sensores via rede sem segmentação adequada (violando princípios da IEC 62443 de conduítes controlados).
  - Impacto: Alteração ou supressão de dados de vibração impede a detecção de falhas críticas, resultando em avarias mecânicas e paradas não planejadas.
  - Técnica: Injeção de dados falsos via gateway IoT comprometido ou uso de credenciais fracas para acesso remoto.

Onde existe um endereço IP conectado a uma rede de controle, existe uma vulnerabilidade

E ainda fica pior – Ataques impulsionados por inteligência artificial

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Weaponized AI for cyber attacks

Muhammad Mudassar Yamin [a,*], Mohib Ullah [a], Habib Ullah [b], Basel Katt [a]

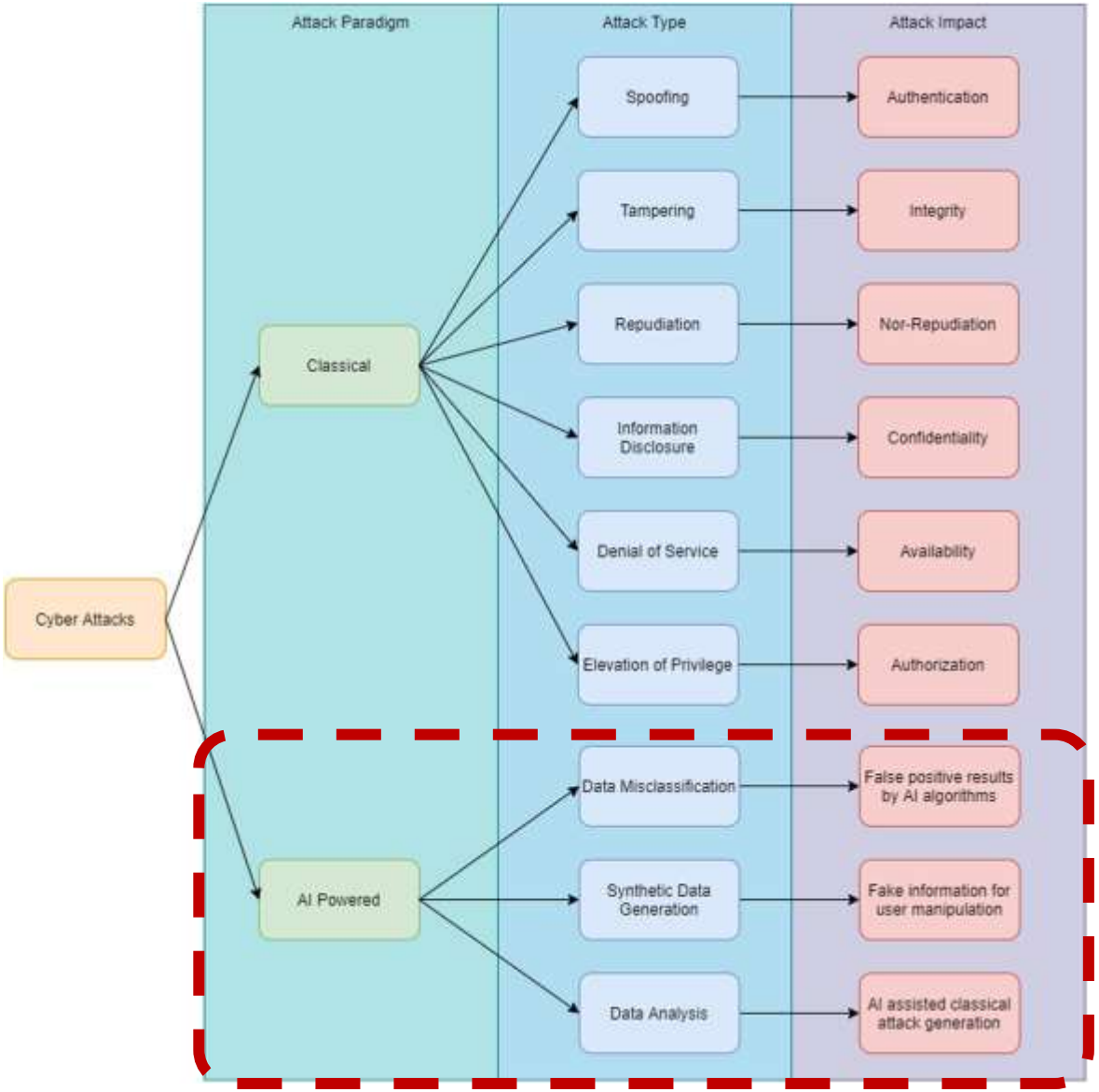
[a] Norwegian University of Science and Technology, Norway
[b] University of Ha'il, Saudi Arabia

ARTICLE INFO

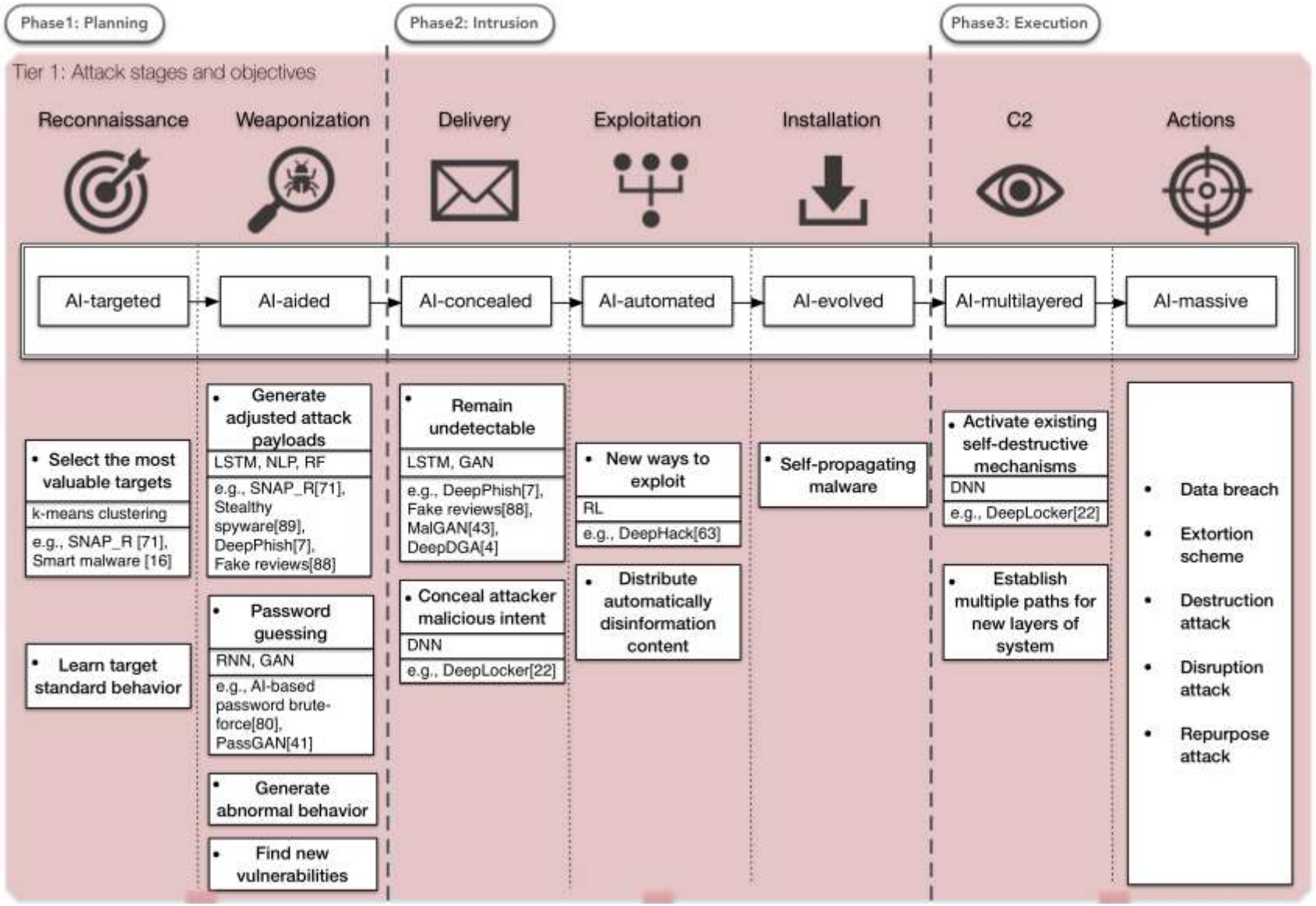
Keywords:
Artificial intelligence
Cybersecurity
Adversarial learning
Scenarios
Cyberattack
Cyber defense

ABSTRACT

Artificial intelligence (AI)-based technologies are actively used for purposes of cyber defense. With the passage of time and with decreasing complexity in implementing AI-based solutions, the usage of AI-based technologies for offensive purposes has begun to appear in the world. These attacks vary from tampering with medical images using adversarial machine learning for false identification of cancer to the generation of adversarial traffic signals for influencing the safety of autonomous vehicles. In this research, we investigated recent cyberattacks that utilize AI-based techniques and identified various mitigation strategies that are helpful in handling such attacks. Further, we identified existing methods and techniques that are used in executing AI-based cyberattacks and what probable future scenarios will be plausible to control such attacks by identifying existing trends in AI-based cyberattacks.



AI-Based Cyber Threat Framework (Nektaria Kaloudi and Jingyue Li. 2019)
Dinâmica dos ataques



CPS requerem defesas avançadas

Componentes do ASCI

Segurança cibernética com IA aplicada

Sistemas de segurança
Origens de alerta

- Firewall
- IDS e sensores de anomalias
- EDR

SIEM
Composição do incidente

- IP, porta. zona de origem
- IP, porta, zona de destino
- Hash, arquivo etc
- Descrição pela origem de alerta
- Correlação baseado no mesmo IP
- Agrupamento por tempo para o mesmo IP

IA especialista (Safer)
Enriquecimento de dados

- Whois
- Virustotal
- Serviços de inteligência
- OSINT
- Histórico de incidentes
- Bases de conhecimento
- Base de chamados

IA + Analista
Abertura do chamado

- Localidade
- Dados do incidente
- Ações recomendadas

CPS-SOC + Equipe local
Resposta ao incidente

- Contenção
- Erradicação
- Recuperação
- Lições aprendidas

Virando o jogo com a Plataforma Safer

Onboarding
480 h de conteúdo

Universidade TI Safe
30+ competências

Base de conhecimento
500+ artigos

Sistema de suporte
150000+ tickets

Eventos de segurança
Bilhões de logs

Incident Hub
2000+ incidentes

Normas e manuais
5000+ páginas

Academia
(Formação e onboarding completos com supervisão e avaliações)

Governança
(Planos e políticas conforme o negócio da empresa gerados 20x mais rápido)

Consultor
(Especialista capaz de avaliar contextos e sugerir soluções com rapidez)

Auditor
(Avaliações de conformidade contra normas de mercado a partir de contextos em segundos)

Analista N1
(Triagem e elaboração de tickets - 95% de redução de falsos positivos)

Analista N2
(Resposta a incidentes - 10x mais rápida)

A nova era da segurança cibernética industrial vai começar!

Plataforma Safer — Lançamento Comercial em Janeiro de 2026

- 🧠 Cibersegurança inteligente com IA e Machine Learning
- 🧱 Plataforma modular com 6 pilares essenciais:
  - Safer.Academia
  - Safer.Governança
  - Safer.Consultor
  - Safer.Auditor
  - Safer.Analista N1
  - Safer.Analista N2
- ⚙️ Conformidade com normas IEC 62443, NIST SP 800-82, RO-CB.BR.01
- 📊 Governança, visibilidade e resposta desde o primeiro mês
- 🌐 Pronta para operadores de CPS, inclusive com recursos limitados

Prepare sua organização para um novo patamar de cibersegurança.

A Plataforma Safer estará disponível comercialmente a partir de Janeiro de 2026.

💡 Solicite uma demo personalizada da Plataforma Safer e conheça a segurança cibernética para CPS com a experiência da TI Safe.

Demonstração da Inteligência da Plataforma Safer

Perguntas para a Plataforma Safer

1. Quais os principais incidentes ocorridos no segmento de petróleo e gás nos dois últimos anos? Poderia listas os 5 mais críticos e escrever uma frase sobre cada um deles?
2. Quais os dispositivos de IoT mais vulneráveis encontrados em plataformas de petróleo? Poderia listar os 5 mais vulneráveis, os riscos envolvidos e como eles podem ser explorados para ataques cibernéticos? Por favor escreva uma frase de até 300 caracteres para cada um destes dispositivos.
3. E na exploração de petróleo onshore, quais seriam estes 5 principais riscos?
4. Poderia me resumir o que sabe sobre o ticket 26717 (Ticket exemplo)
5. Poderia redigir um plano de ação para este incidente?

Perguntas do público ----- perguntem o que quiserem!

Obrigado!

TiSafe

www.tisafe.com

Marcelo Branquinho
marcelo@tisafe.com