Prime

CCS-A

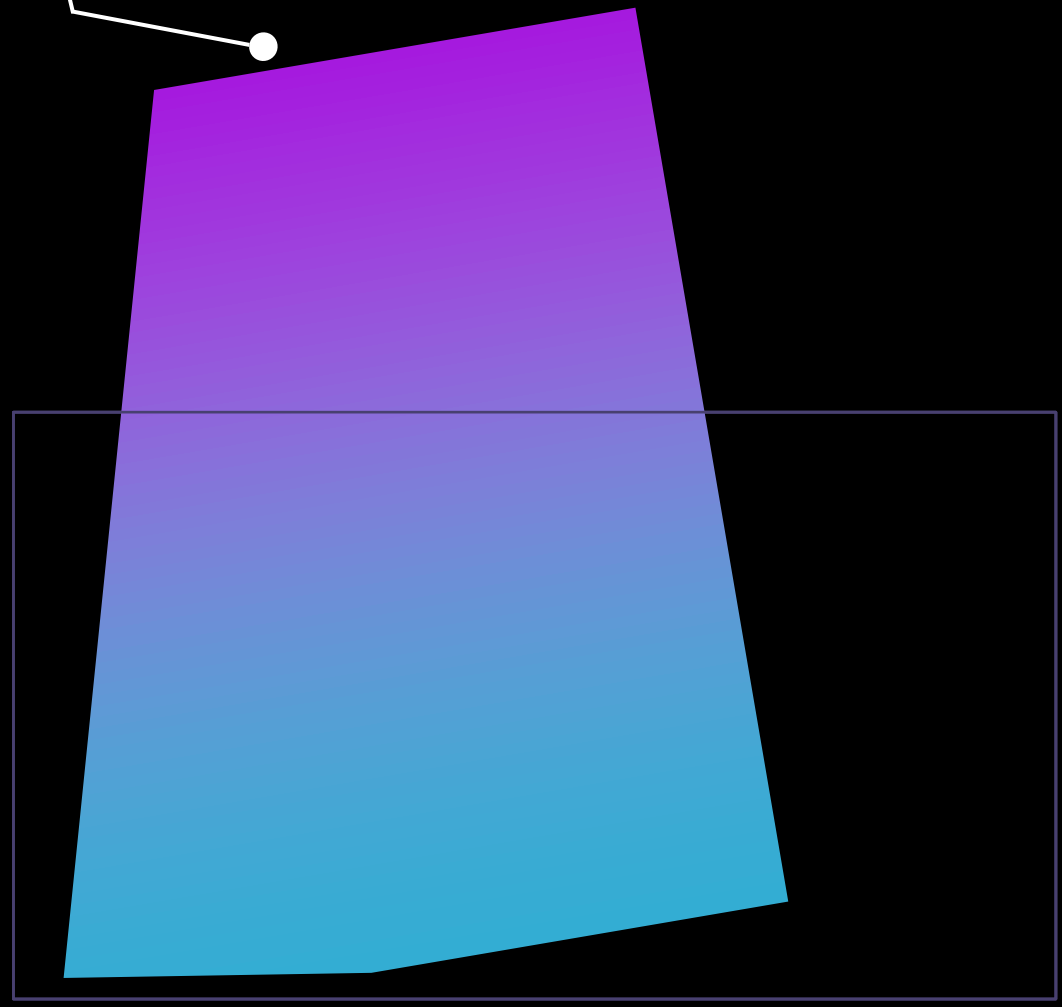
Sistemas Embarcados e Especializados

Sistemas Embarcados

- Computadores incluídos como parte de um sistema maior.
- Alguns exemplos:
  -  Impressoras ou Smart TV;
  -  Dispositivos domésticos que tenham Bluetooth;
  -  Carros inteligentes.
- As explorações de segurança estão presentes em vários aspectos: rede, hardware, conectividade, atualização etc.
- A medida que os sistemas se conectam em rede, aumentam os riscos.

Raspberry Pi

- Computador de placa única de grande sucesso e baixo custo.
- Oferece recursos, conectividades e USB e HDMI.
- Plataforma versátil.
- Proteger um Raspberry Pi é como proteger um sistema.
- Determinar os perfis de risco e tratá-los é importante.



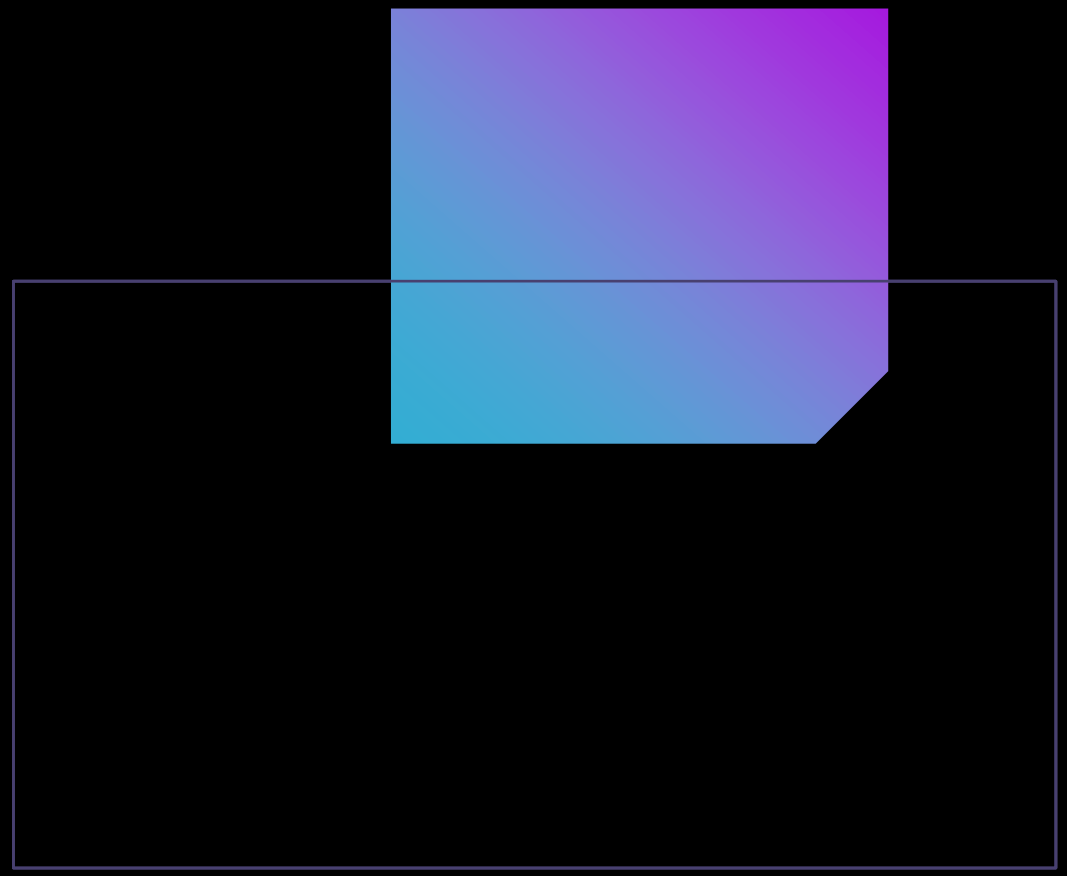
Matrizes de Portas Programáveis em Campo (FPGA)

Circuitos eletrônicos programados para executar uma função. É uma extensão do microprocessador.

Projetos para serem reprogramados após a fabricação, dando maior poder.

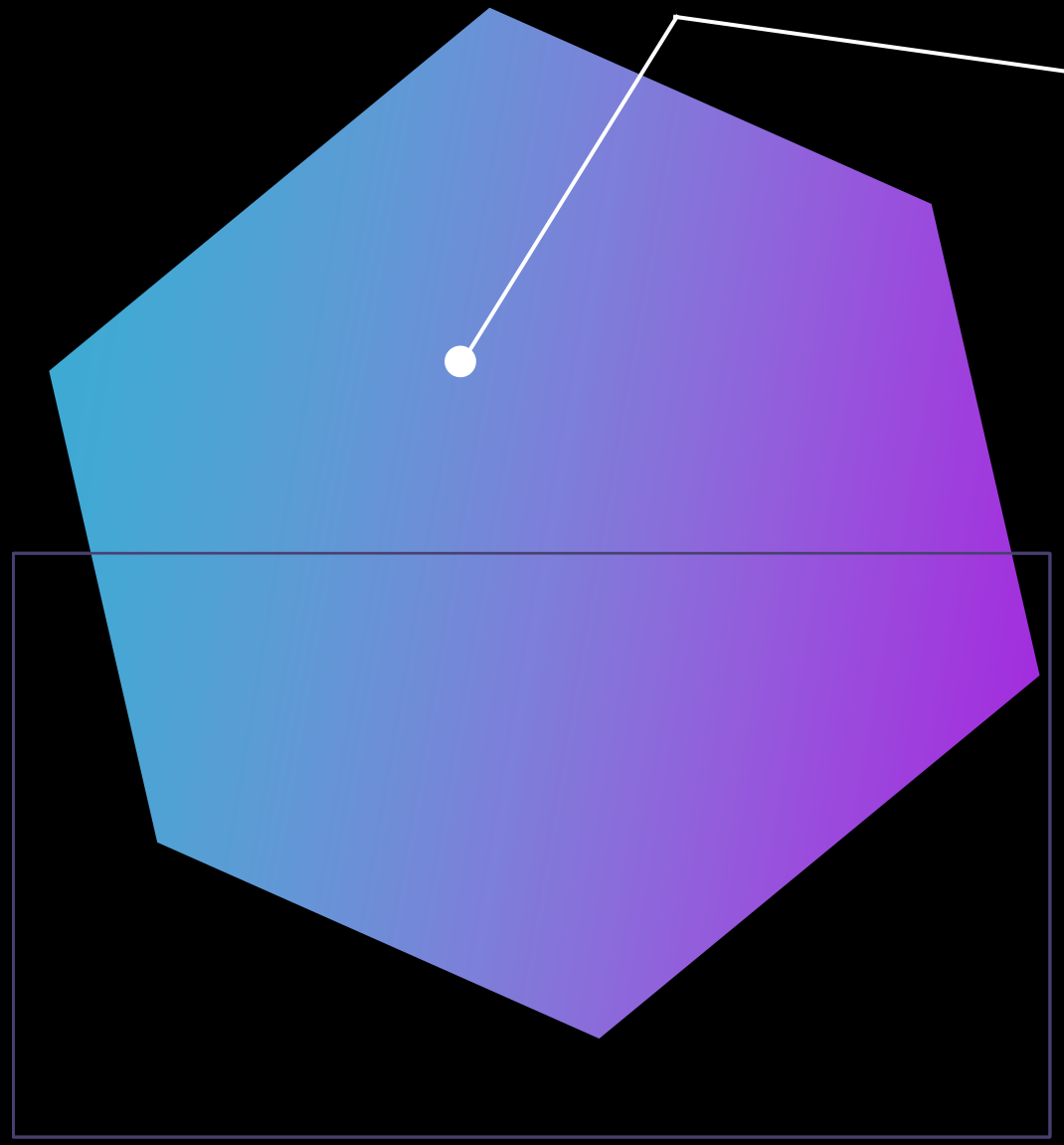
Podem ser reprogramados conforme os projetos evoluem.

FPGAs e ASICs são encontrados em muitos dispositivos.



Arduino

- Microcontrolador de placa única.
- Mais simples e bem popular.
- Projetado como um controlador de dispositivos.
- Responde a níveis de sensores e aciona dispositivos.
- Aciona dispositivos com base na programação que é carregada.
- A expansão é feita através de placas (escudos) para novas funcionalidades.



Sistema de Supervisão e Aquisição de Dados (SCADA) / Sistema de Controle Industrial (ICS)

- SCADA – Controle de Supervisão e Aquisição de Dados usados em:
  -  Fábricas;
  -  Semáforos;
  -  Refinarias;
  -  Redes de energia;
  -  Usinas hidroelétricas;
  -  Automação predial;
  -  Controles ambientais.
- Sistema de Controle Industrial (ICS) controla e monitora o SCADA.
- Sistemas SCADA ficaram famosos graças ao Stuxnet.

Instalações do SCADA

- SCADA é utilizada em muitas instalações.


Automação predial;


Bombas de pressão de água;


Escadas rolantes;


Elevadores;


Alarmes de incêndio.

Ambientes Industriais

Qualquer instalação pode ter um sistema de coleta de dados, seja um termostato ou alarme.

Podem ser autônomos.

Podem ser parcialmente integrados.

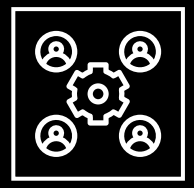
Podem ser conectados à Internet.

Manufatura

Sistemas usados no próprio processo de fabricação real.

Comumente controlados por computador, graças aos equipamentos de Controles Lógicos Programáveis (CLPs).

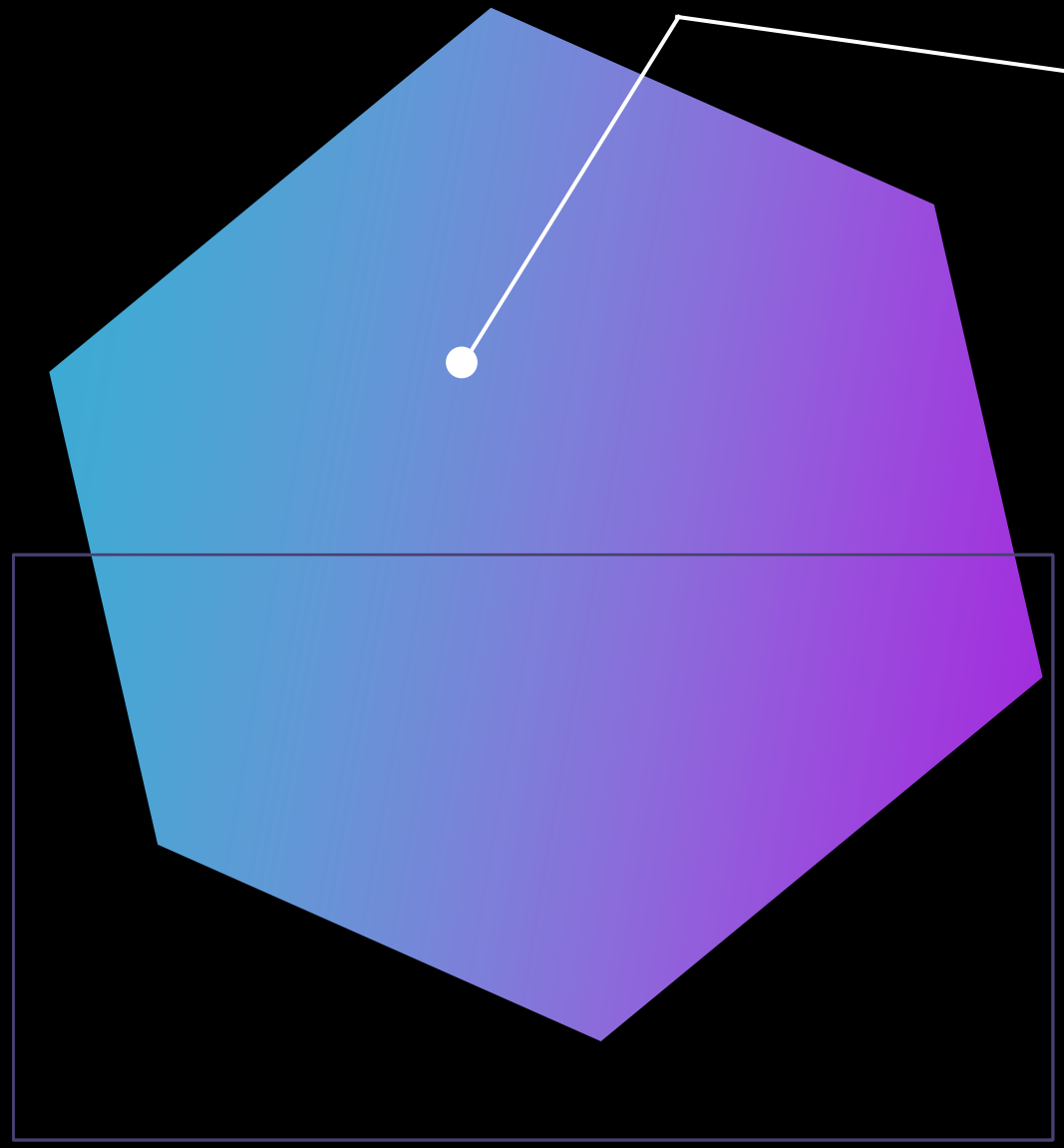
Podem estar conectados à Internet.



Devem ser protegidos contra invasão, como a segmentação de uma rede restrita.

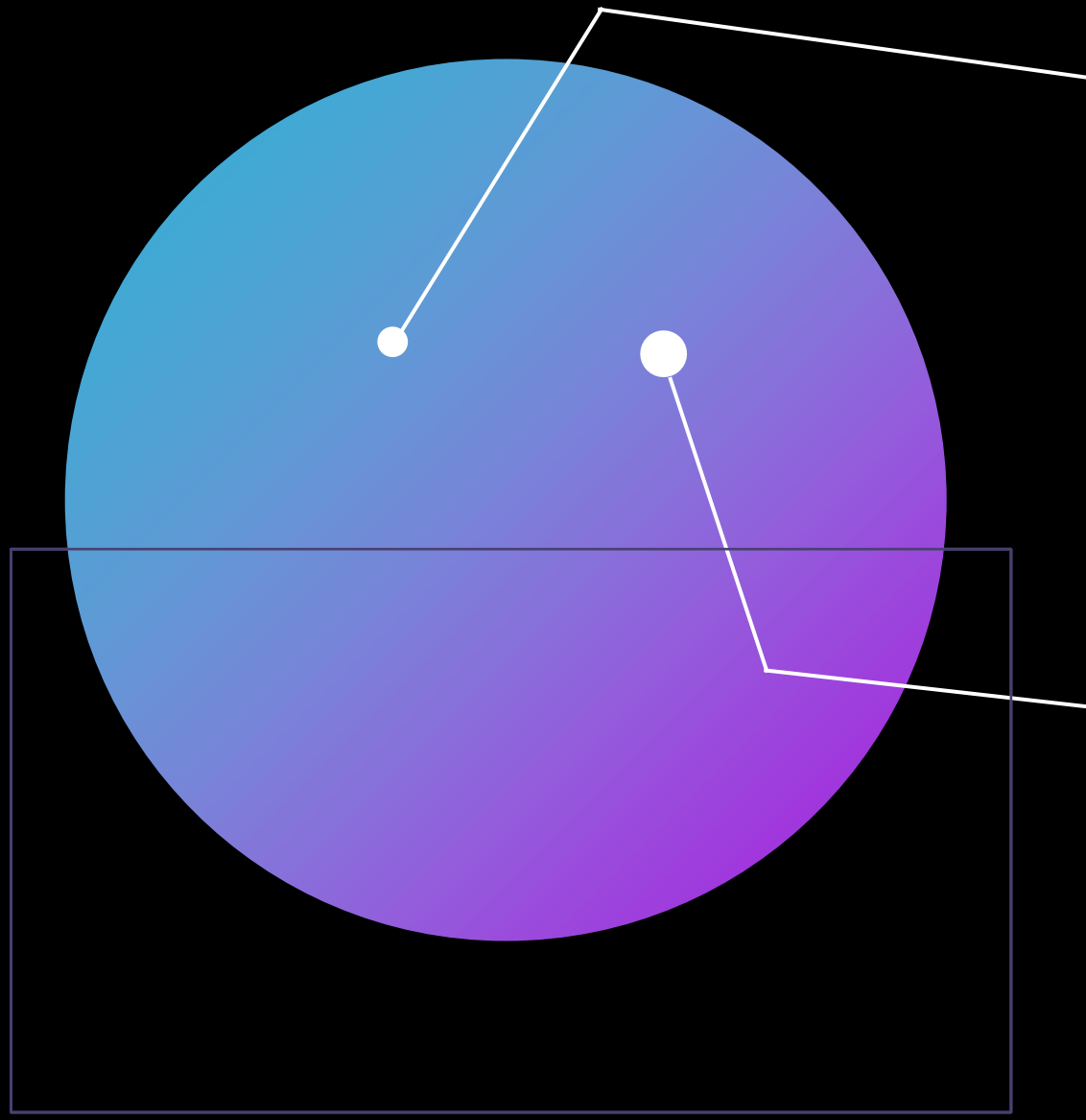
Energia

- Variam de:
  - Elétrica;
  - Química;
  - Petróleo;
  - Gaseoduto;
  - Nuclear;
  - Solar;
  - Hidrotermal.
- Podem ser inseguros por estarem fora dos “muros coorporativos” e inseridos na comunidade.



Sistemas Logísticos

- Sistemas que movimentam um material do ponto A ao B.
- Podem envolver:
  - Transporte marítimo;
  - Transporte terrestre;
  - Transporte aéreo.
- Dois elementos básicos que estarão sob controle:
  - O próprio sistema de transporte;
  - Material que está em movimento.

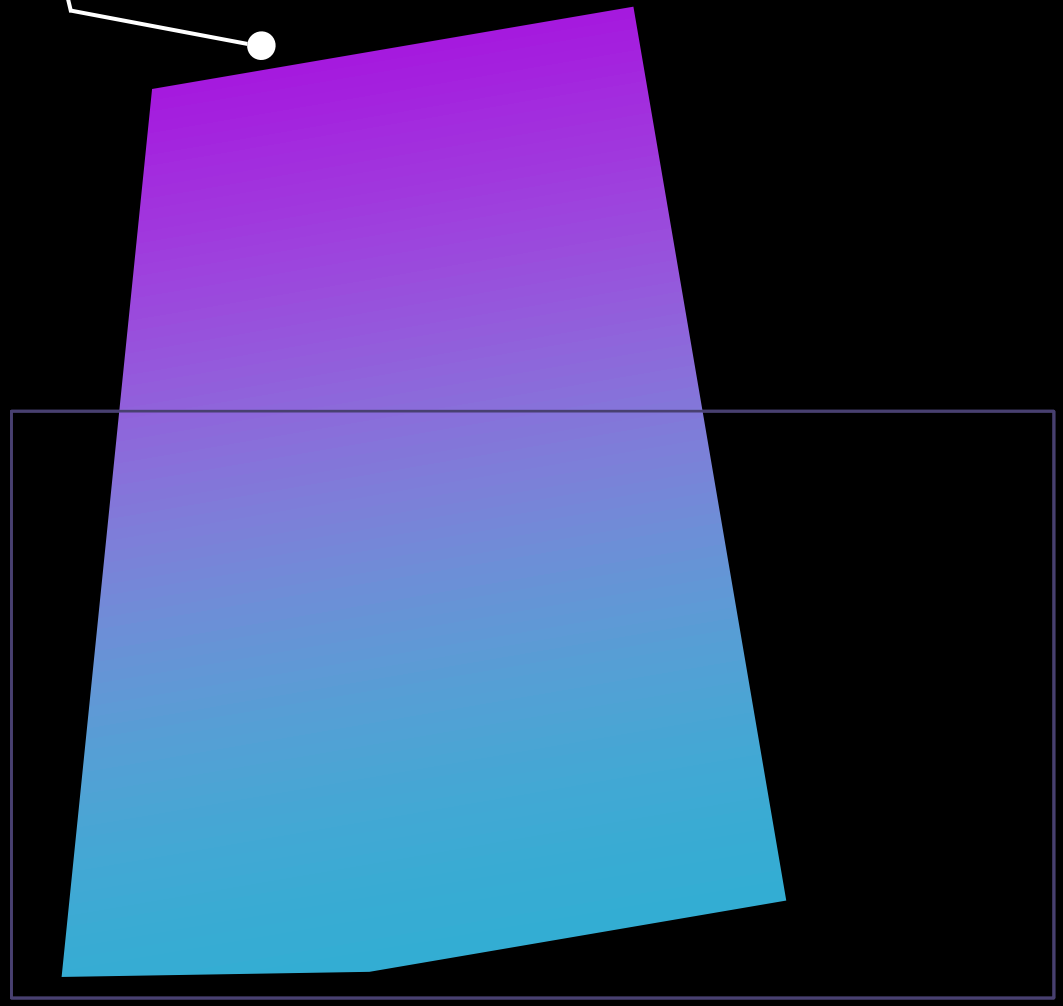


Internet das Coisas (IoT)

- Ampla gama de dispositivos que se conectam na Internet e criam um sensor distribuído e um sistema de processamento.
- Construídos com usos específicos.
- Possuem algumas semelhanças entre si:
  - Interface de rede;
  - Alguma forma de plataforma de computação;
  - Computador completo em funcionamento: baratos;
  - Uso de kernel do tipo Linux, facilitando a programação.
- Exemplo de falha: Malware Mirai (2016).

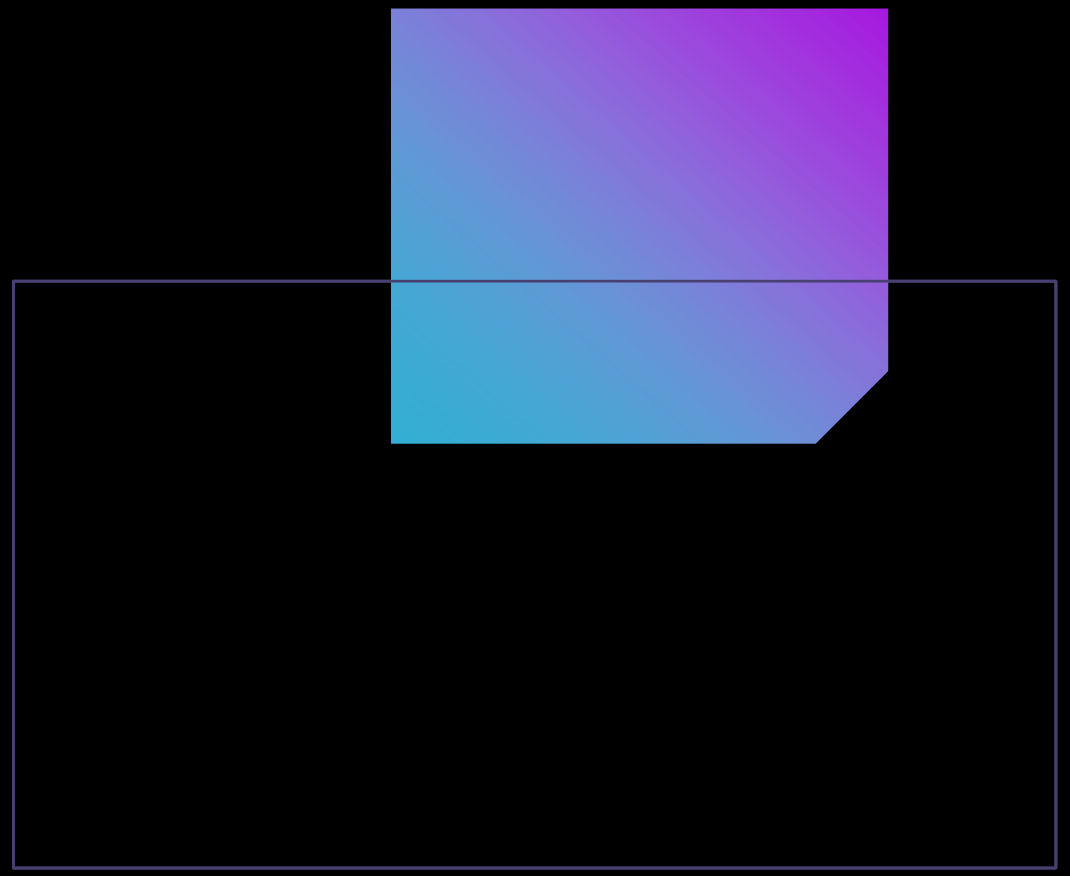
Sensores

- Dispositivos que medem e coletam dados de algum item físico.
- Podem ser usados para medir:
  - Temperaturas;
  - Pressões;
  - Voltagens;
  - Posições;
  - Níveis de umidade.
- É preciso determinar o que precisa ser medido, para ajudar no custo de aquisição e especificações.



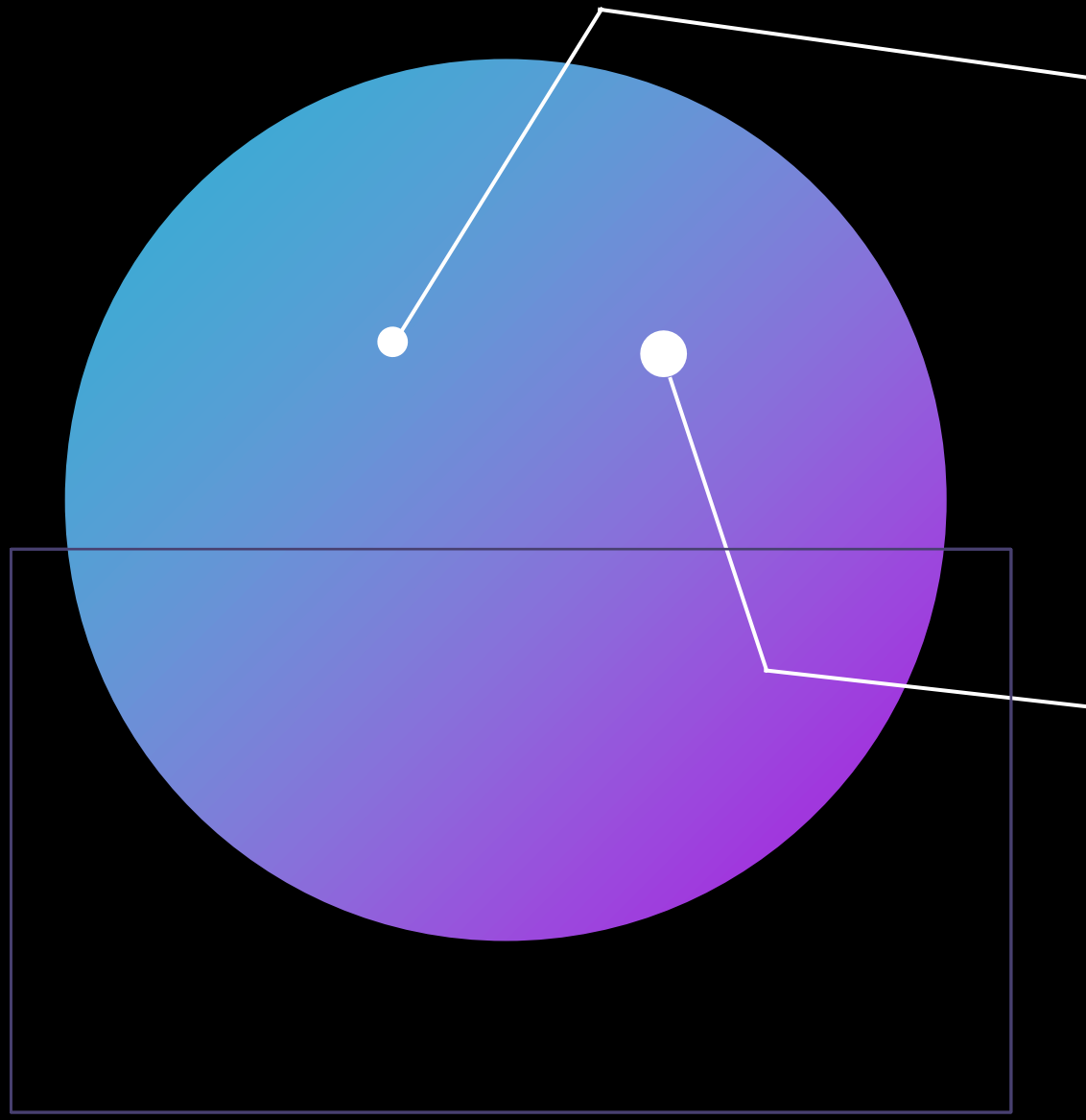
Dispositivos Inteligentes

- Chaveiros que rastreiam itens;
- TVs;
- Geladeiras;
- Lavadoras;
- Interruptores de luz controlados;
- Termostatos;
- Casa inteligente.
- Câmeras;
- Lava-louças;
- Panelas elétricas;
- Secadoras;
- Lâmpadas LED;
- Babás eletrônicas;



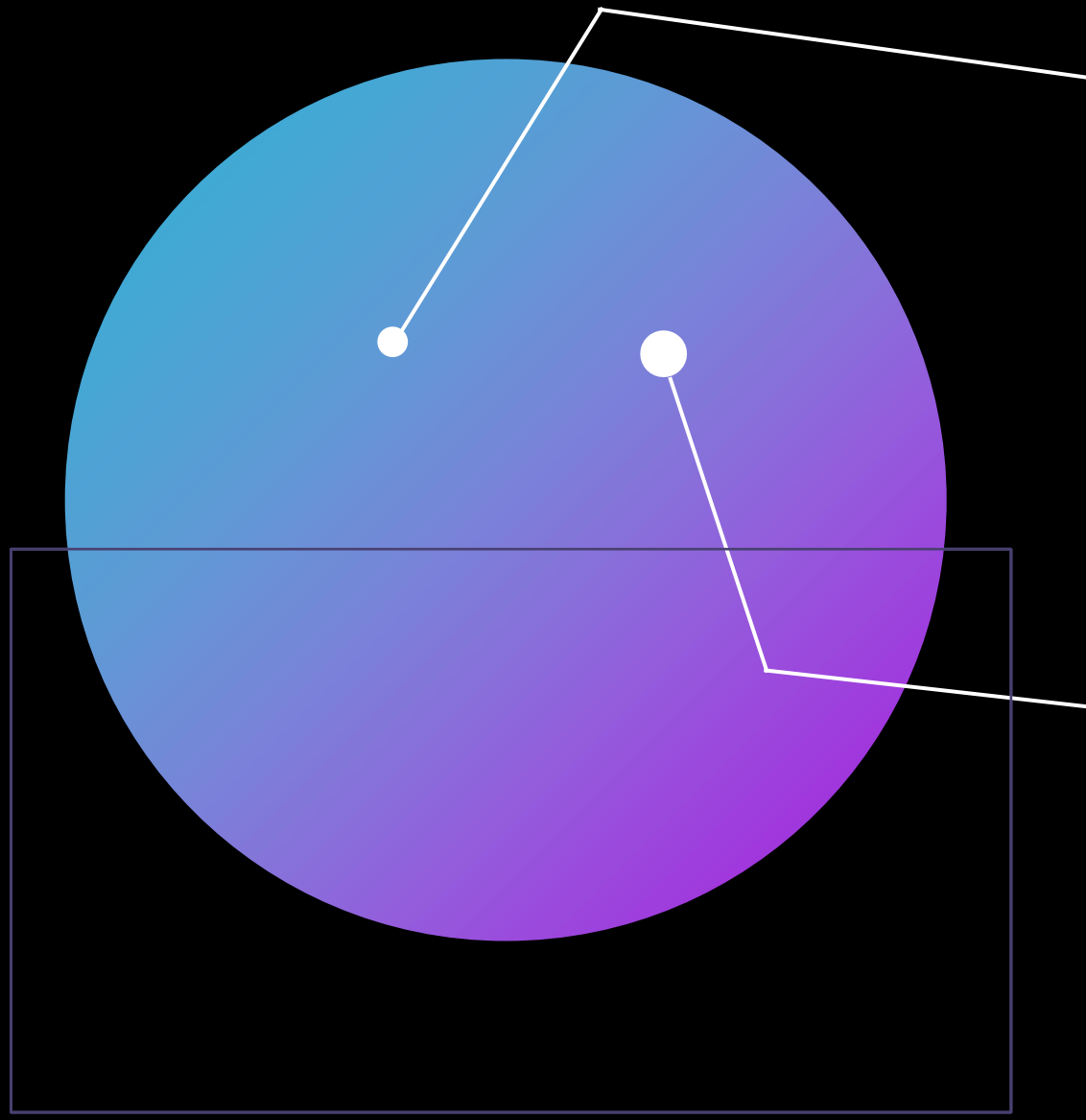
Wearables

- Tecnologias vestíveis:
  - Sensores biométricos;
  - Contadores de passos;
  - Relógios inteligentes;
  - Muito mais.
- Utilizam computadores muito pequenos.
- Quanto mais usados e dados gerados sobre o usuário, mais atenção recebem de hackers.



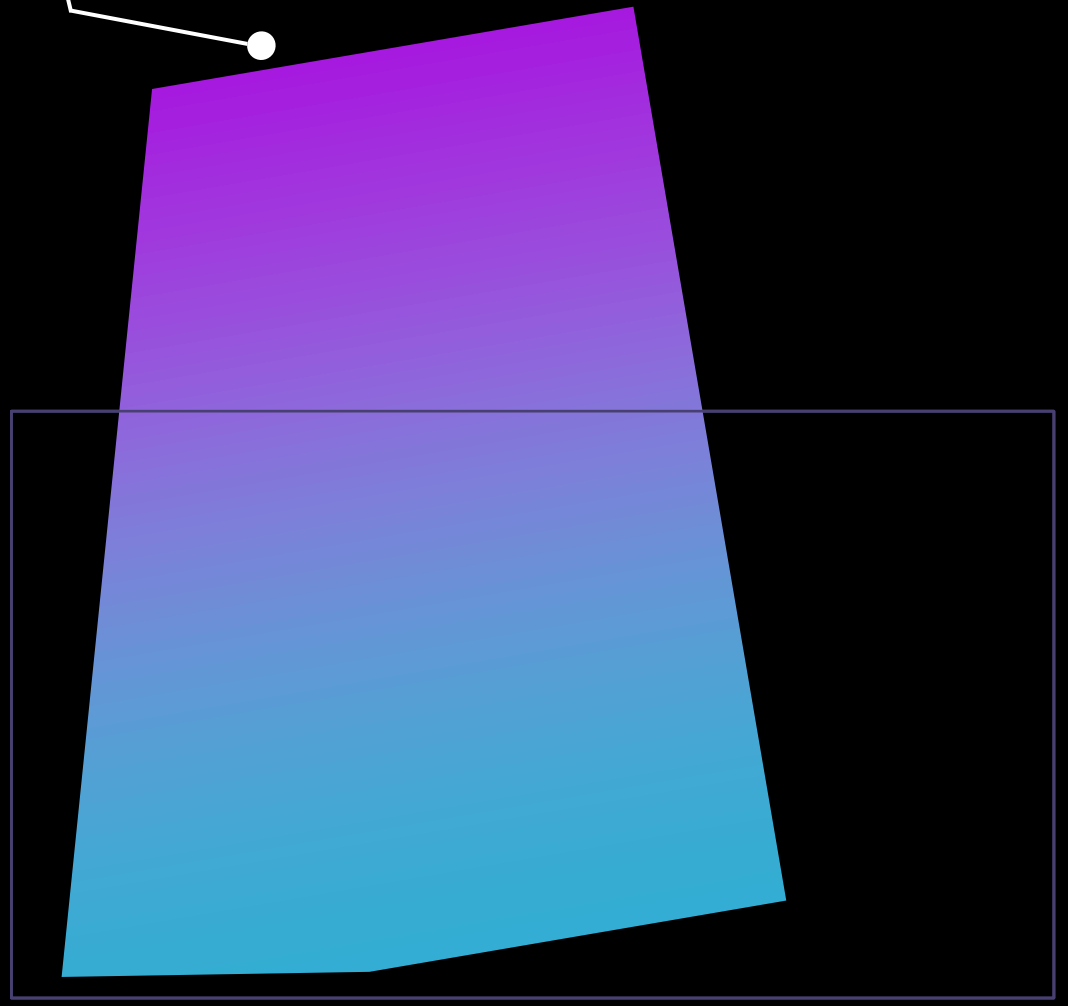
Protegendo Wearables

- Verificar:
  - Configurações padrão;
  - Configurações de privacidade;
  - Desativar o rastreamento de localização;
  - Ler políticas de privacidade;
  - Usar senha para PII.



Automação das Instalações

- Vantagens de IoT de HVAC, incêndio, luz etc.:
  - Automação na coleta de dados.
- Automação é mais do que operação remota.
- Sistemas IFTTT podem responder a mudanças de condição e usar vários indicadores.
- Benefícios da Automação:
  - Remove riscos de erros;
  - Melhora a velocidade.

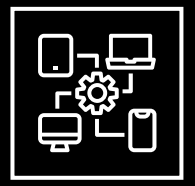


Configurações Padrão Fracas

Especificações como credenciais é um desafio. Foco na usabilidade e não na segurança.

Padrões Fracos: Alteração de credenciais de fábrica, username = admin e senha = admin.

Outras configurações padrão são o que os hackers conhecem.



Desafio para implantação e segurança do IoT: Gerenciar milhares/milhões de dispositivos.

SISTEMAS EMBARCADOS E ESPECIALIZADOS

Sistemas Médicos

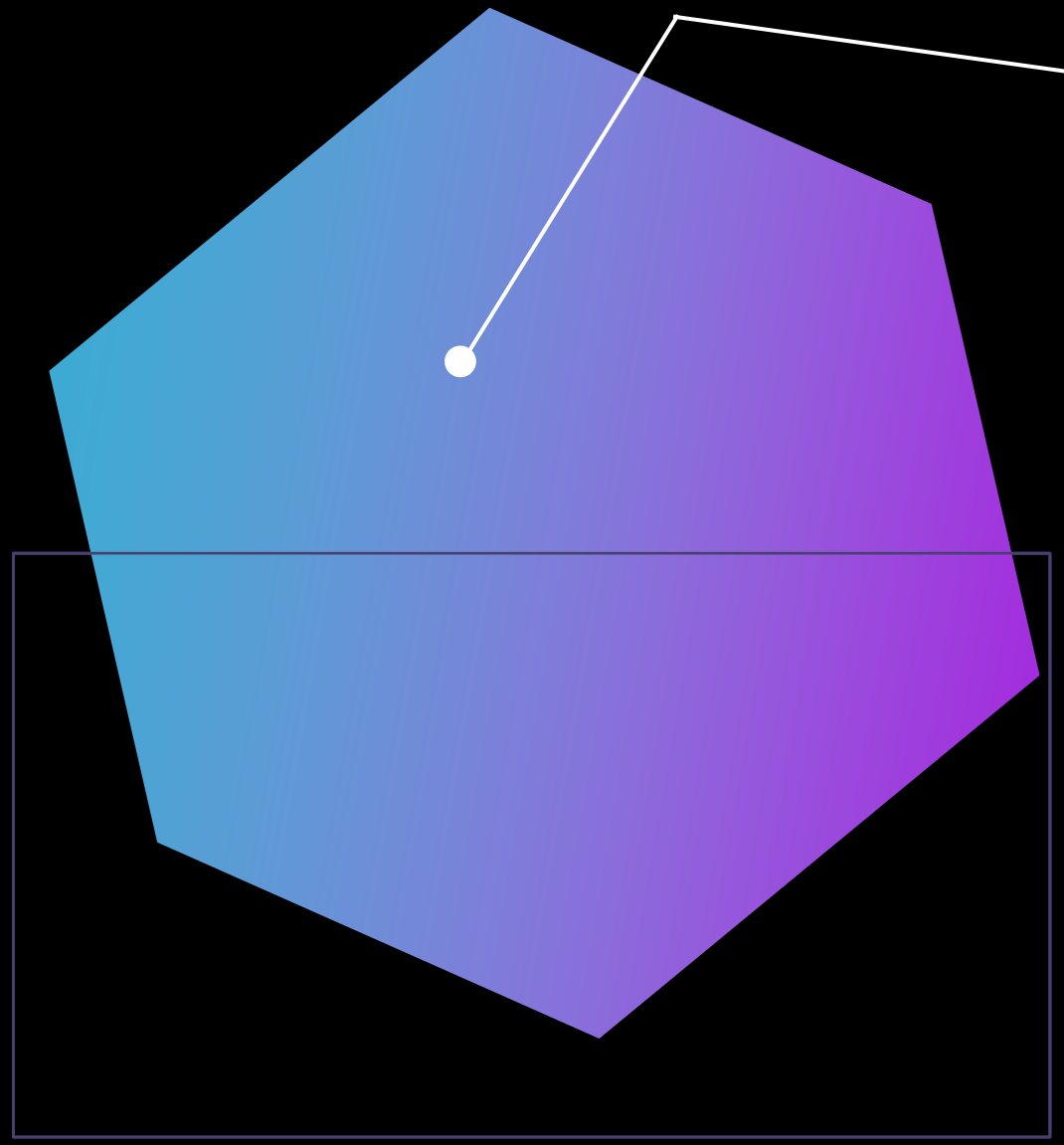
- **Sistemas especializados** – Projetados com propósitos especiais.
- Sistemas Médicos - Exemplos:
  - De dispositivos implantáveis;
  - Até máquinas de ressonância magnética.
- Podem ter um efeito direto na vida do ser humano.
- Padrão de escolha: kernel Linux.
  - Problemas: Atualização do sistema básico e coleta de dados sensíveis.
  - **Exemplo:** Recall de quase meio milhão de marca-passos em 2017 exigiu visita ao médico para atualização do firmware.

Sistemas de Veículos

- Veículos modernos possuem centenas de computadores interligados e controlados centralmente (CAN).
- Antigamente os microcontroladores eram separados.
- Descoberta de hackers:
  -  Aceleração repentina sem a ação do motorista;
  -  Controle quase completo do veículo quando hackeado;
  -  Desativação do carro em movimento;
  -  Controle das configurações do console de entretenimento.
- Veículos dependem de vários sistemas de computador, que por vezes não tem muita segurança.

Sistemas de Aeronaves

- Com Cockpit de Vidro que é mais moderno e confiável.
- A conexão de todos os equipamentos levou a muitas questões de segurança.
- Corrigir o sistema operacional de aeronaves é um processo difícil, pois:
  - Setor com requisitos rigorosos de teste;
  - Com o tempo, os sistemas ficam vulneráveis.
- Perigo: sistemas de entretenimento são separados dos controles de voo apenas por um firewall (não físicos).

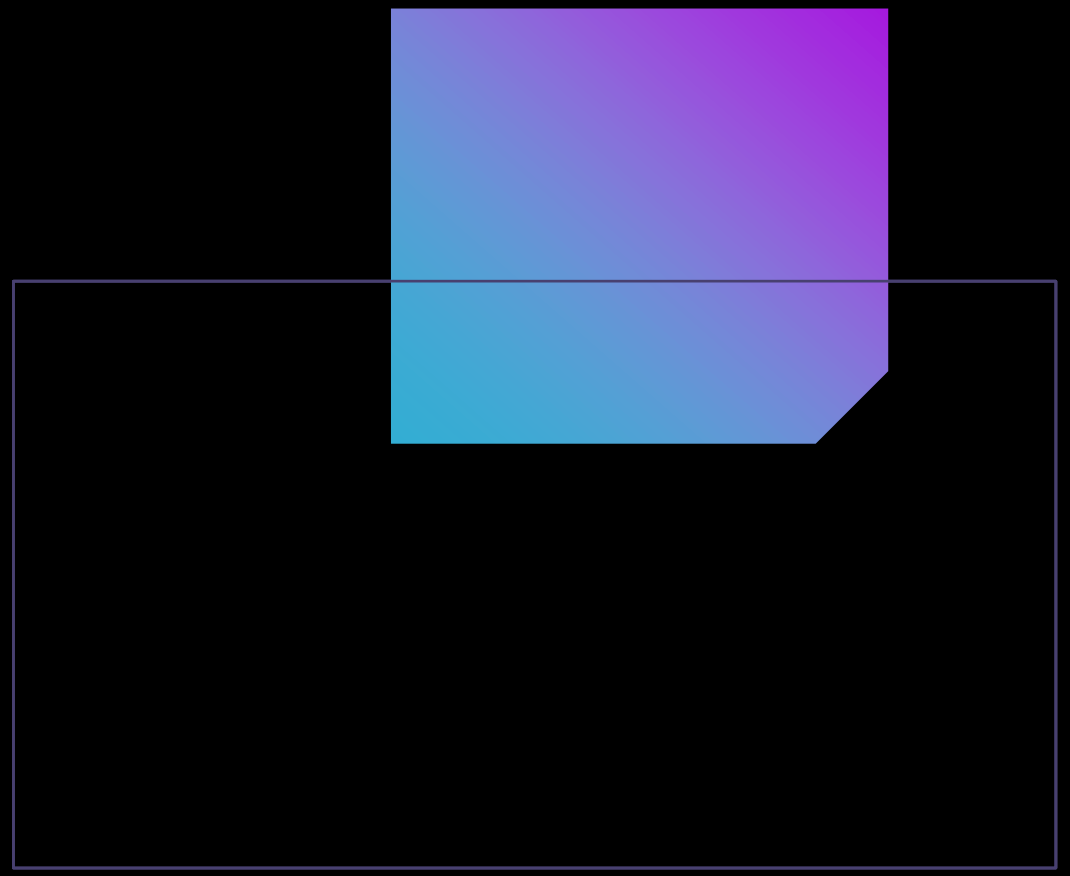


Medidores Inteligentes

- Infraestrutura de medição e coleta avançada de energia.
- Isso foi permitido com:
  - Comunicações bidirecionais;
  - Infraestrutura para análise de dados;
  - Novas políticas e procedimentos para automação.
- Para concessionária, energia são dados de uso em tempo real.
- Permite a combinação de oferta e demanda.
- Gerenciar a infraestrutura em larga escala requer uma configuração criptográfica (os medidores tem senha).

Voice Over Internet Protocol (VoIP)

- Transmissão de comunicações de voz sobre redes IP.
- Método comum para serviços telefônicos.
- Exigem proteção contra ataques em tráfego (DoS e falsificação).
- Riscos adicionais:
  - Pessoas de fora usando seu VoIP para:
    - Conectar a serviços de telefonia internacional;
    - Oferecer chamadas telefônicas gratuitas;
    - Usar seu serviço para chamadas automáticas.

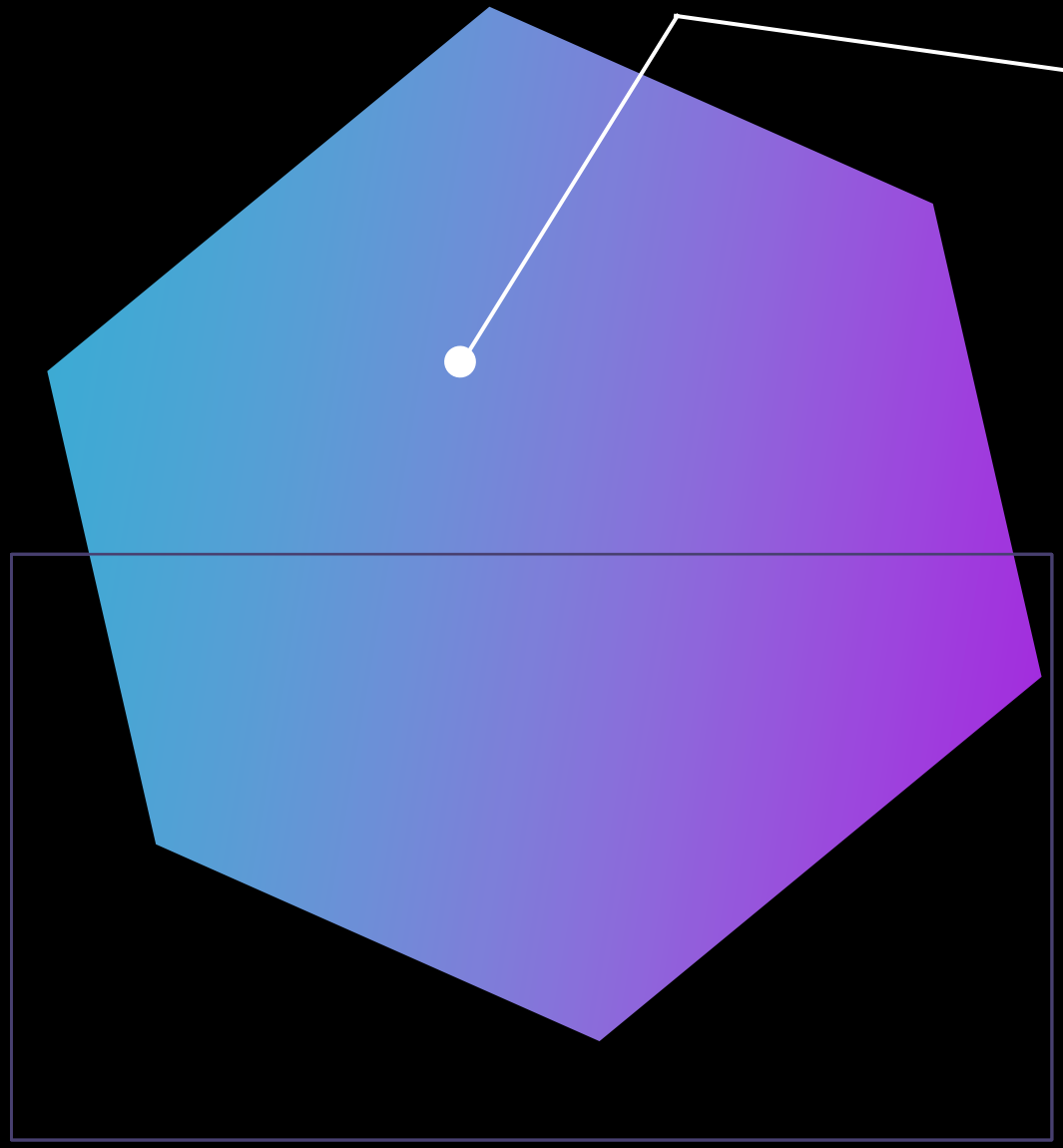


Heating, Ventilation and Air Conditioning (HVAC)

- Exemplo de sistema embarcado.
- Conectividade e integração aos sistemas de automação predial e controle climático.
- Edifício inteligente = Controle de recursos.
- O controle é baseados na Internet aumentando o risco a ataques externos.
- Ataques podem fazer um prédio fica inabitável devido o calor e segurança.

Drones

- UAVs representam a próxima fronteira do voo
- Variam de pequenos a verdadeiras aeronaves.
- Diferença: o piloto está no solo.
- Possuem:
  - Câmeras;
  - Sensores;
  - Processadores;
  - Piloto automático.
- Conectados em rede e operados por rádio ou por sistema em rede.

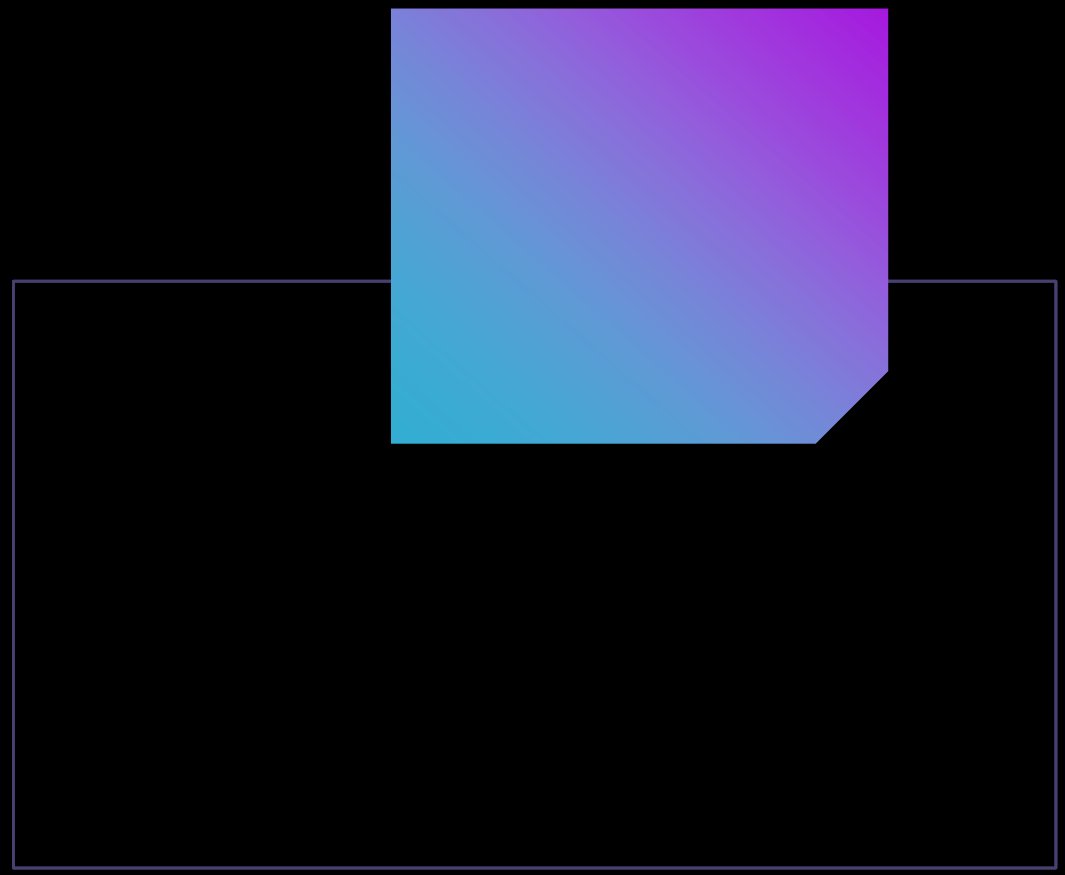


Impressoras Multifuncionais (MFDs)

- Combinam:
  - Impressora;
  - Scanner;
  - Fax.
- Comunicam-se de maneira bidirecional.
- Projetadas para fornecer o máximo de funcionalidade e não tanto de segurança.
- Podem transmitir malware da impressora para o computador.

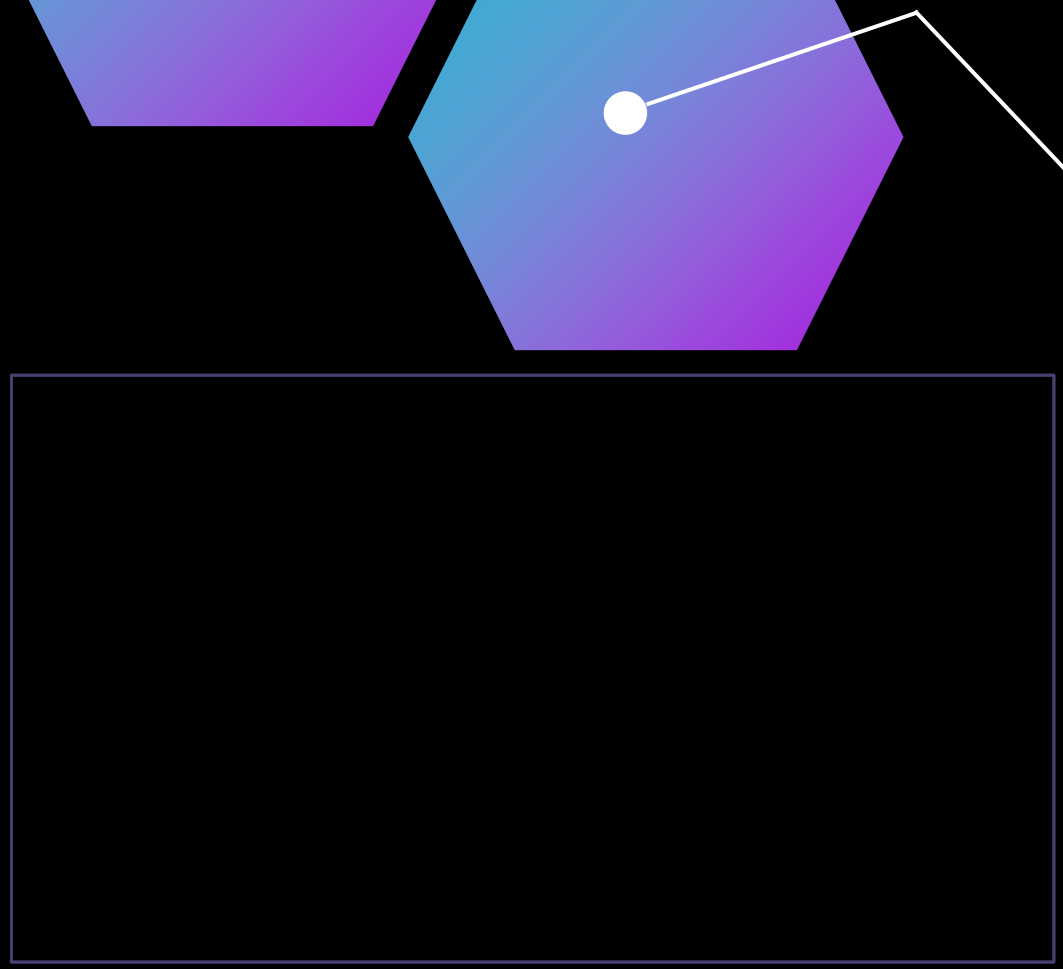
Sistemas Operacionais em Tempo Real (RTOSs)

- Projetados para dispositivos com processamento em tempo real.
- Os dados não podem ser enfileirados ou armazenados em buffer.
- Processa a entrada à medida em que é recebida.
- Exemplos:
  - Sistema de frenagem antitravamento;
  - Sistema robótico em uma fábrica.
- Escrito para enfatizar o encadeamento no processamento e não multitarefa.
- Problemas:
  - Falha no sistema devido a alguma interferência;
  - Tendência a serem específicos e, consequentemente, sem atualizações e patches.



Sistemas de Vigilância

- Câmeras digitais de última geração, além de:
  - Pilhas de rede;
  - Processadores de imagem;
  - Feeds de vídeo 4K.
- Possuem Redes Privadas Virtuais (VPN).
- As câmeras de vigilância incluem:
  - Vigilância doméstica;
  - Monitoramento de bebês.



Sistema-Em-Um-Chip (SoC)

- Sistema de computador completo em um único circuito integrado.
- Comuns no mercado de computação móvel.
- Já possuem sistemas mais avançados, em quadcore e oito núcleos.
- SOs e aplicativos dedicados podem ser escritos para eles (fork Android do Linux).
- Incluem CPUs, GPUs e módulos sem fio.
    - Exemplo de dispositivo que usa um SoC é o Raspberry Pi

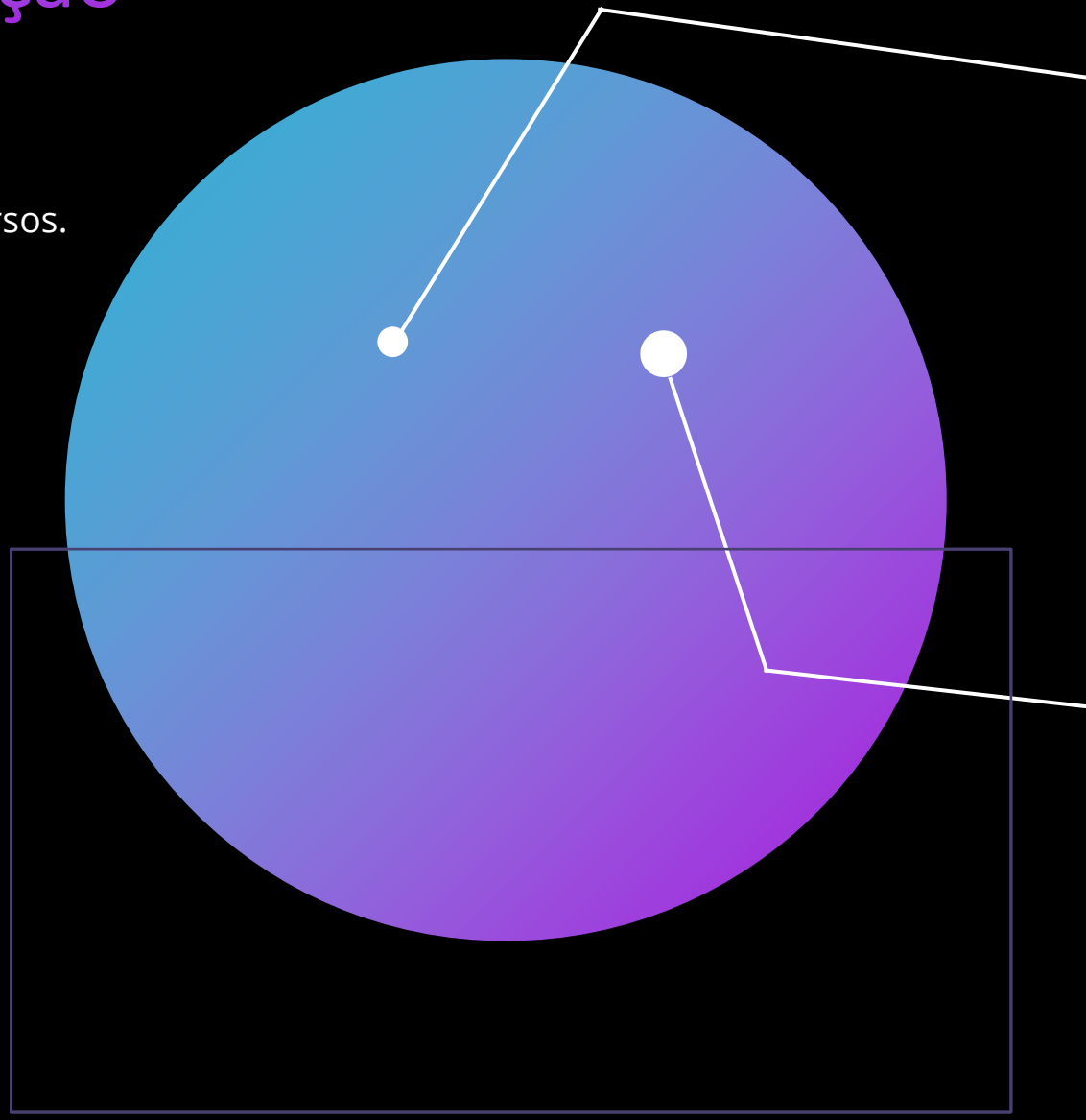
Considerações Sobre Comunicação

Sistemas embarcados e especializados requerem comunicações através de uma rede para outros recursos.

Métodos de comunicação são amplos.

Também pode variar de acordo com a localização.

Adotar tecnologia já empregada por usuários também traz vantagens.

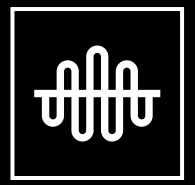


5G

- Rede móvel baseada em rádio de última geração.
- Conecta praticamente tudo e todos juntos:
  - Máquinas;
  - Objetos;
  - Dispositivos.
- Melhora o desempenho e a eficiência.
- Pode ser um exagero para muitas necessidades de comunicação.

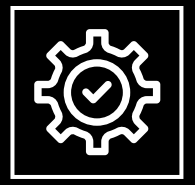
Rádio de Banda Base

O termo Banda base serve para descrever a frequência original de uma transmissão antes da modulação.



Utiliza a onda de rádio para ser transportado..

Usa ondas de rádio para enviar um sinal entre dois pontos.



Mais simples. Exemplo de sinal de rádio banda base seria: código Morse.

Rádio de Banda Estreita

Usam bandas estreitas de frequências para comunicações de baixa taxa de dados.

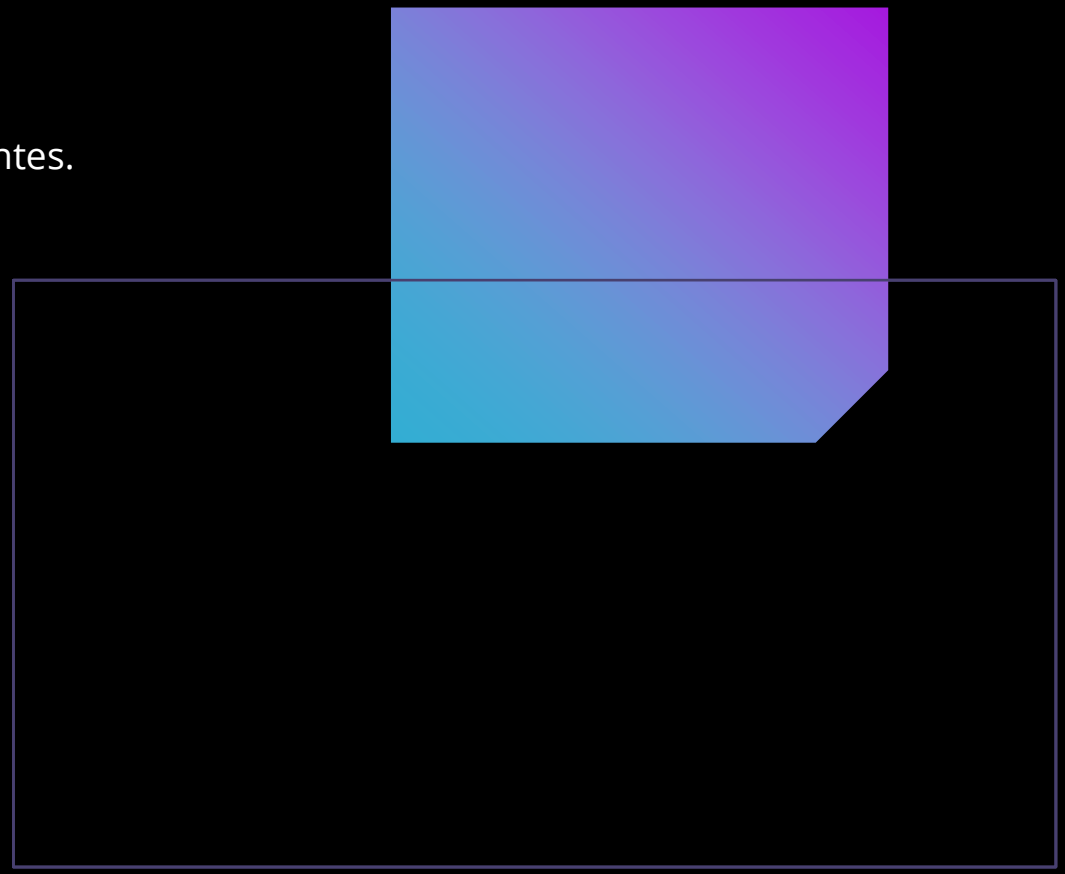
Nem todos os sistemas têm necessidades de alta taxa de dados.

Oferece vantagens de alcance baixo e energia.

São usados transmissores de baixa potência, como RFID e controle remoto de carro.

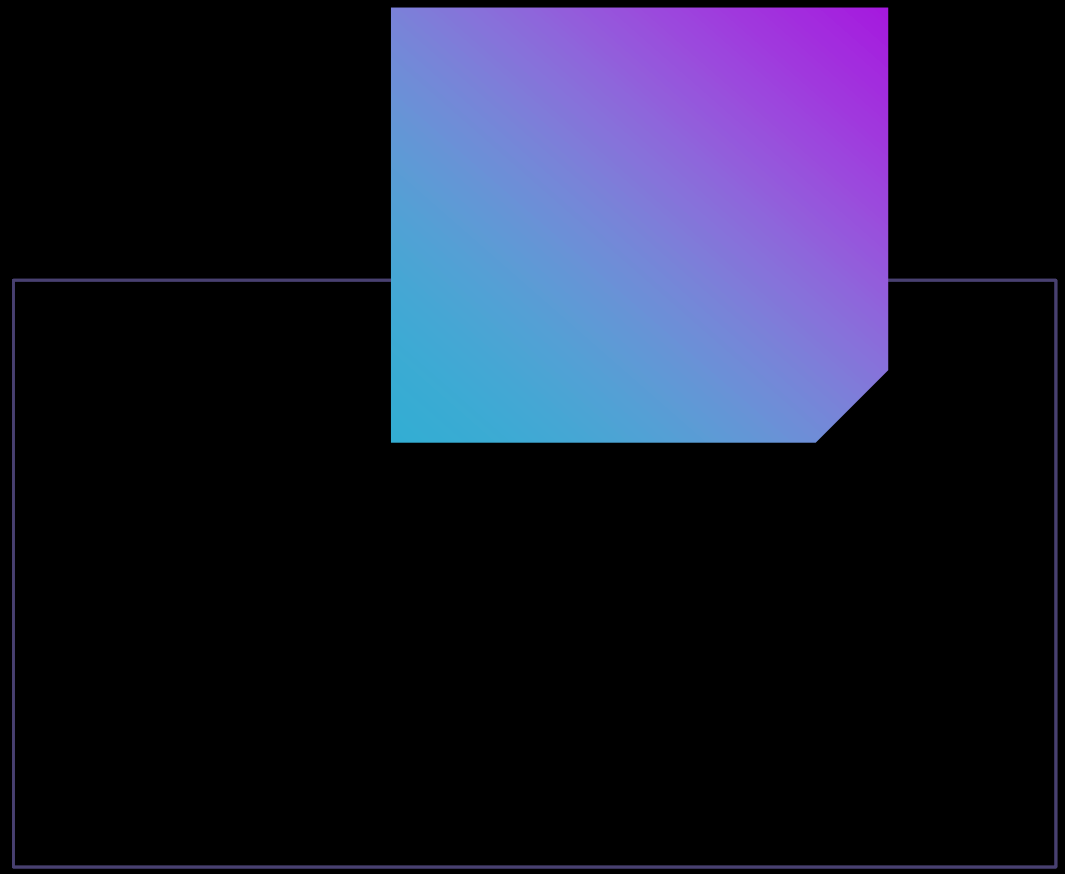
Cartões SIM e Zigbee

- Dispositivo que armazena as informações necessárias para conduzir comunicações em redes de telecomunicações.
- Fornece um meio de identificar usuários e outros itens importantes.
- Fornece informações necessárias para atribuir a chamada.
- Armazena elementos como:
  - Provedor;
  - Números de série;
  - Chaves.



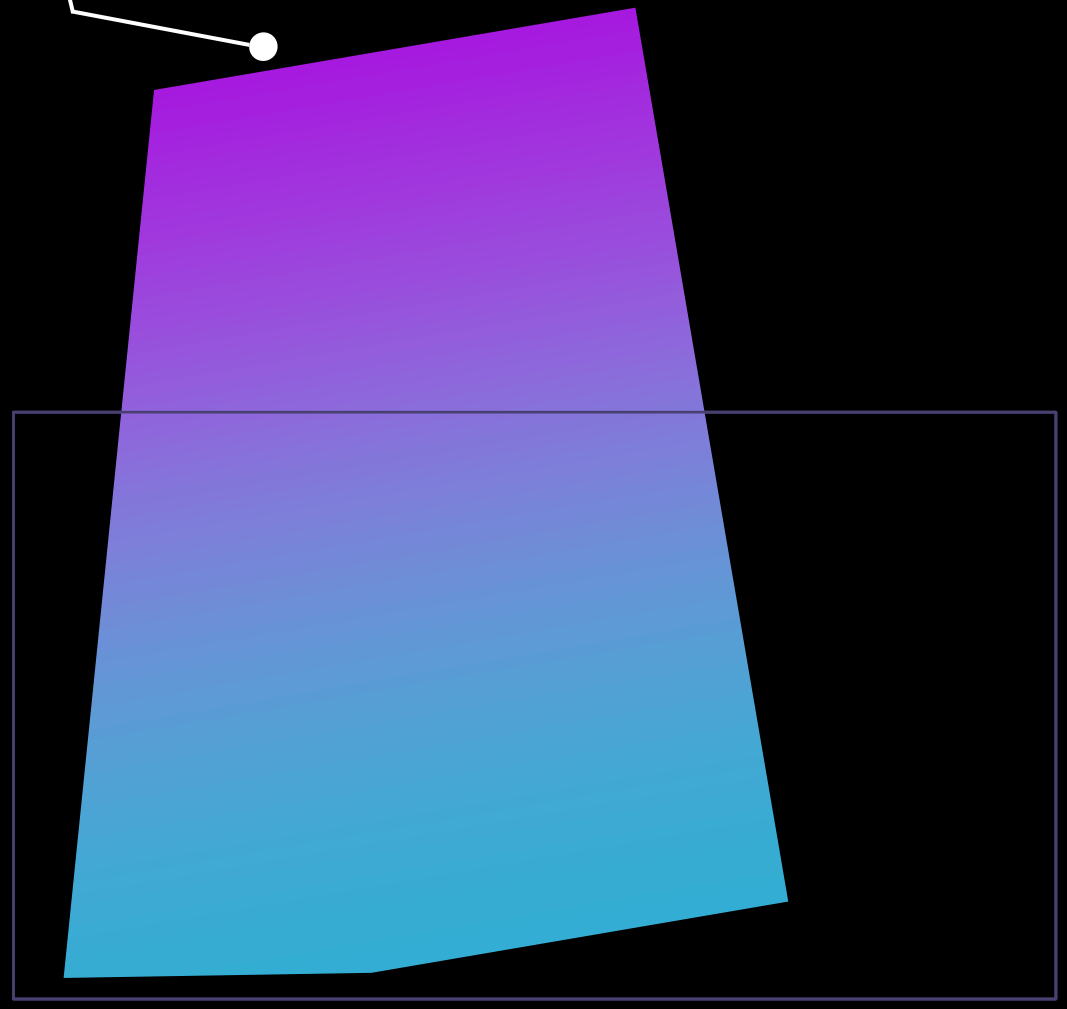
Cartões SIM e Zigbee

- São importantes porque podem conter:
  - Dados de usuário;
  - Autenticação;
  - Informações.
- **Zigbee** - Serviço de rádio mesh de baixa potência para uma rede pessoal e residêncial.



Restrições

- Sistemas especializados e embarcados possuem restrições.
  - Limitações de energia;
  - Capacidade de computação;
  - Taxa de transferência;
  - Largura de banda da rede;
  - Criptografia;
  - Custo;
  - Autenticação;
  - Confiança.



Energia

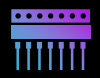
- Circuitos eletrônicos consomem energia de várias fontes:
  - Alimentação conectada à rede;
  - Bateria;
  - Energia solar;
  - Outros tipos de dispositivos.
- Quando não há backup, o dispositivo para de funcionar.
- Fonte primária: Baterias recarregáveis de íon de lítio.

Computação

- Depende da capacidade de computação de sistemas embarcados e especializados.
- Um dos elementos principais na equação de energia.
- Resulta em mais consumo de energia e menos vida útil com a carga de bateria, caso haja excessos.
- Para projetar a computação:

Microcontroladores;

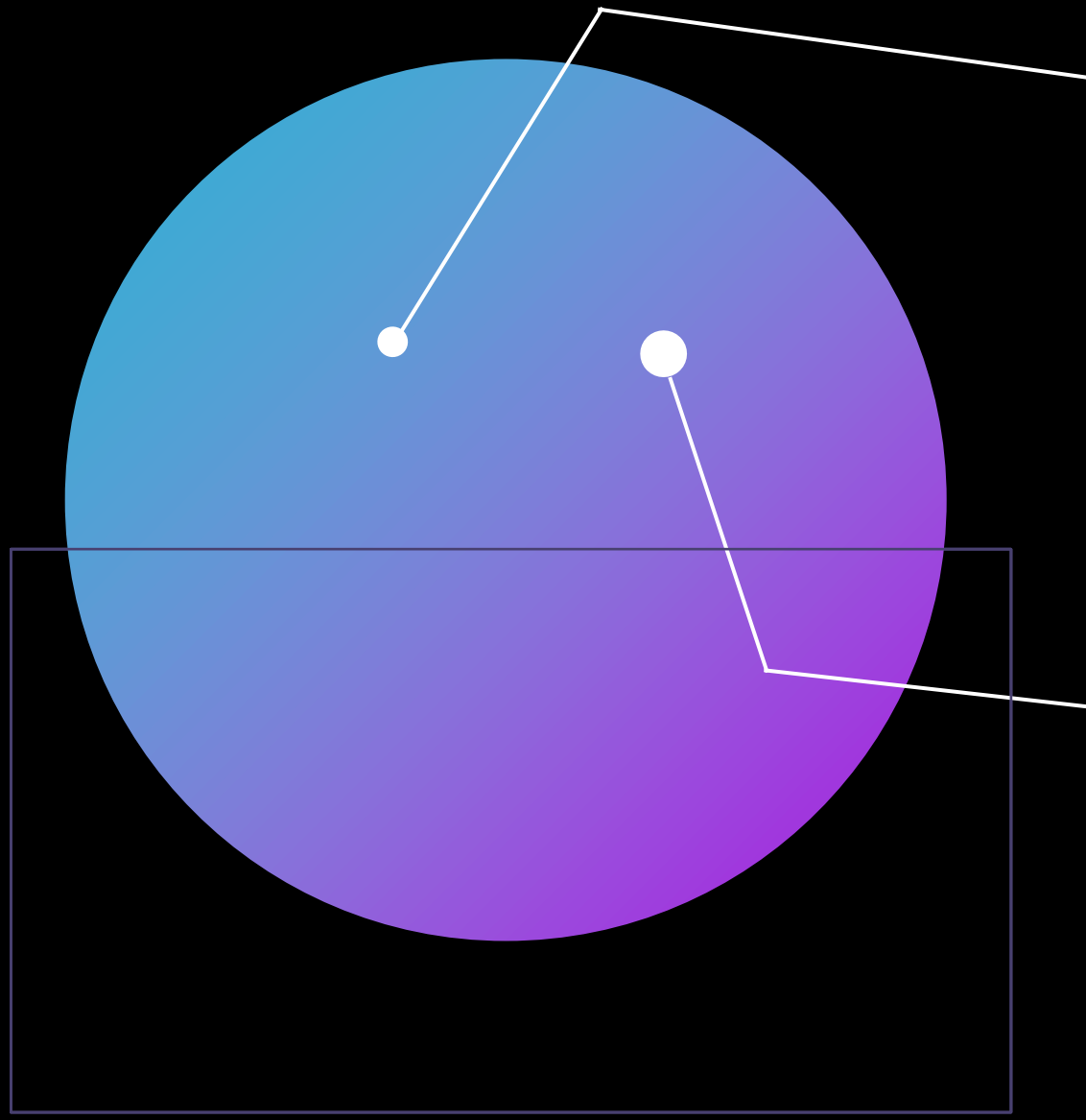
Matrizes de portas programáveis em campo (FPGAs);



Circuitos integrados específicos de aplicativos (ASICs).

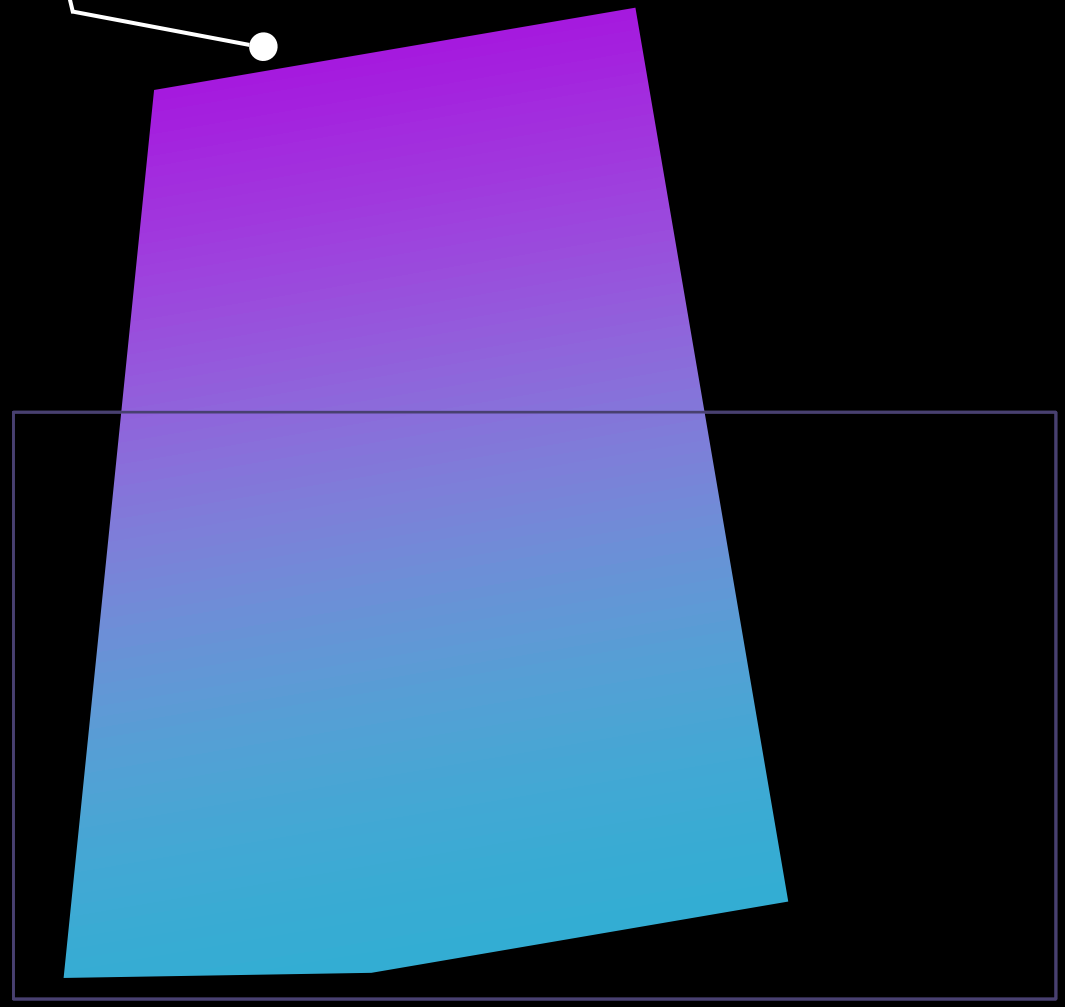
Rede

- Limitações:
  - Restrições de energia;
  - Conectividade.
- Onde há rede, há custo de dados e energia.
- Principal componente de valor para o IoT.
- Quanto mais nós, mais útil é a rede. O crescimento é de natureza exponencial.
- Grandes fluxos de dados sobrecarrega o site central.



Incapacidade de Correção

- Causada por uma série de decisões de design.
- Rasberry Pi e Arduino recebem paches de correção, já uma câmera de vigilância, por exemplo....
- Ecossistema de dispositivos embarcados muitas vezes não têm:
  - Meios de atualização;
  - Cultura de segurança;
  - Capacidade de gerenciar o processo de correção.



Autenticação e Criptografia

Confidencialidade e integridade deve constar nos termos de usuário. Busque soluções para criptografar a comunicação.

Há problemas em adotar o conceito de autenticação criptográfica.

Sistemas especializados e embarcados tendem a desempenhar uma função singular se o usuário é indefinido.

É preciso uma interface administrativa para algumas funções.

Alcance, Custo e Confiança Implícita

Alcance – Bluetooth 4.2 é limitado a 60 metros, enquanto o Zigbee, o máximo é 100 metros.

Custo - Funcionalidade extra leva a um custo extra para o cliente.

Confiança Implícita - Facilita a conectividade ao mesmo tempo em que abre portas para um invasor.

OBRIGADO!

SISTEMAS EMBARCADOS E ESPECIALIZADOS