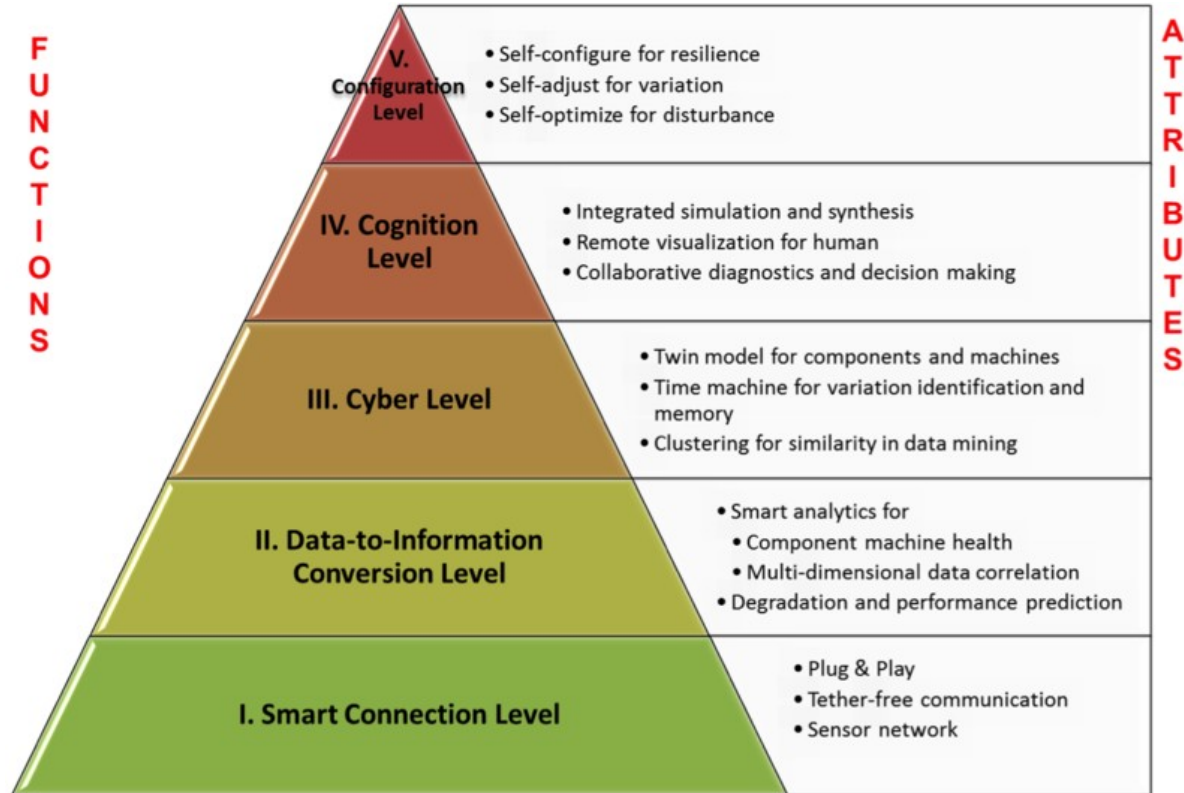


Introdução ao IIoT

Dispositivos e segurança -

Daniela Maria Uez
dani.uez@gmail.com

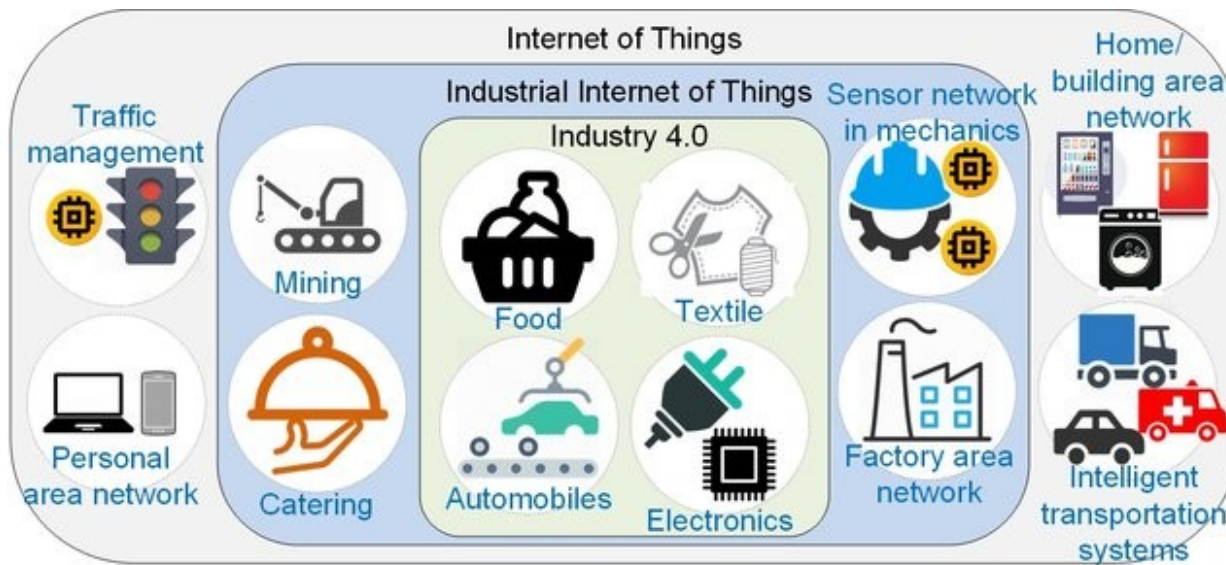
Arquitetura 5C



IoT / IIoT

IoT : Internet of things - Objetos + habilidade de “sentir e comunicar”

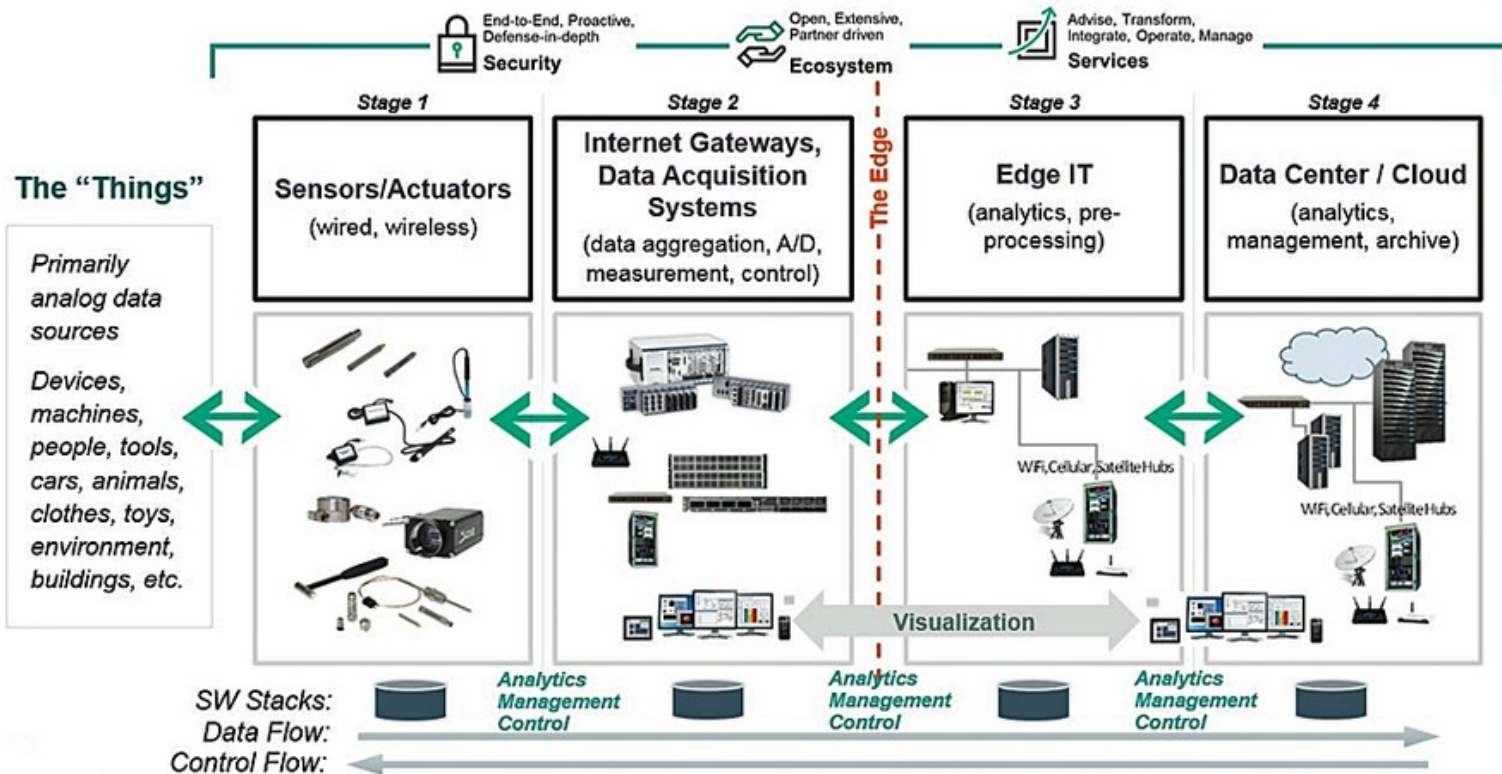
IIoT: Industrial Internet of things - IoT para objetos industriais



Fábrica conectada



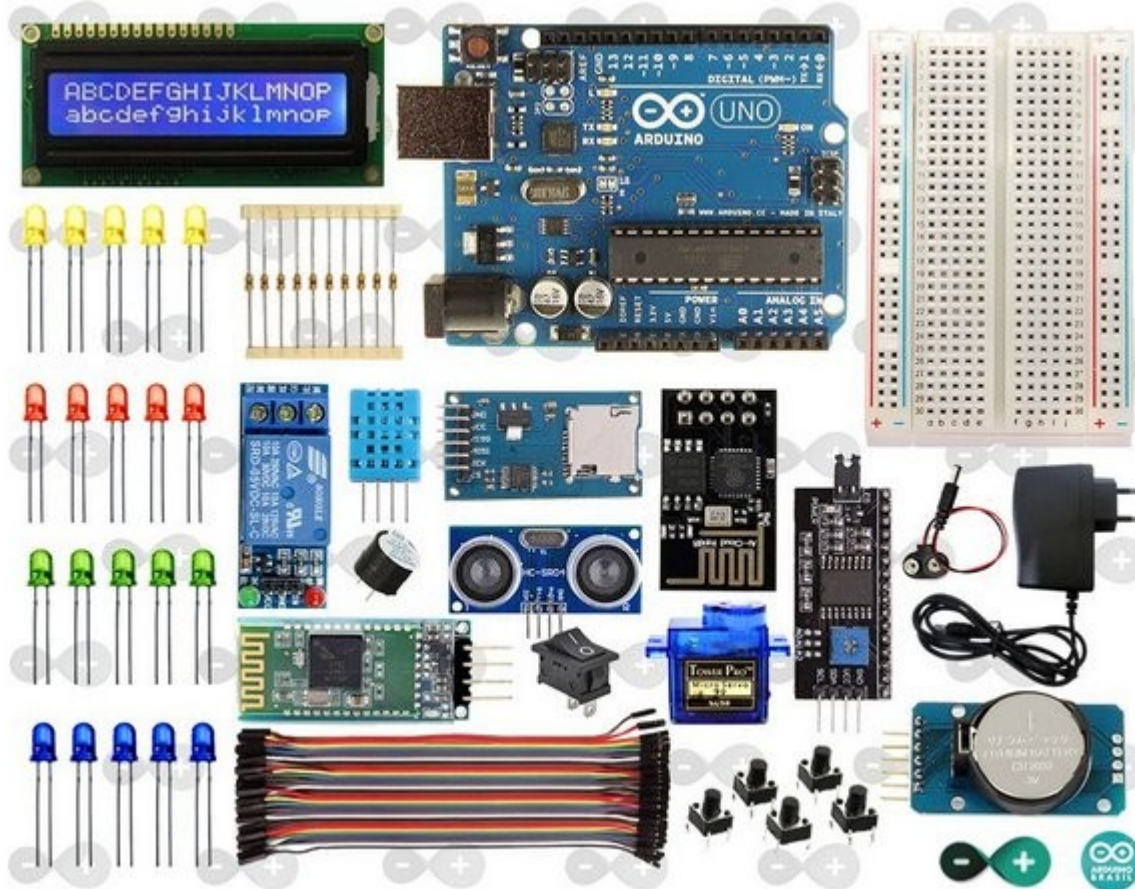
IIoT – Arquitetura



Hardware – System on Chip (SOC)

- Sistemas eletrônicos integrados a um microcontrolador (MCU) que podem ser programados
 - Possuem inputs/outputs de propósito geral
 - Normalmente usam memória permanente (SDRAM)
- Mais popular é o Arduino
 - Pode ser programado através do Arduino IDE

Arduino



Hardware (II)



- Controles lógicos programáveis (PLC)
 - Um microcontrolador “gigante”
 - Faz o mesmo que um microcontrolador pode fazer mas com maior velocidade, performance e segurança
 - São mais utilizados para controle local
- Unidades de terminais remotos (RTU)
 - Dispositivo eletrônico de controle com microprocessador
 - Permite controlar objetos reais
 - Altera o status de objetos conectados e transmite dados através de mensagens de controle
 - São mais utilizados para grandes áreas

PLC e RTU

- Programmable Logic Controller (PLC)
- Remote Terminal Unit (RTU)



Hardware – Single Board Computer (SBC)

- Um “computador completo” imbutido in uma placa de circuito
 - Possui memória, micorprocessadores, I/O e outras características de um computador comum
- Usados principalmente para sistemas educacionais ou como computadores embutidos
- Raspberry Pi: criado para ensinar os conceitos básicos de ciência da computação nas escolas e muito usado para robótica e projetos de IoT
- Omega – criado pela startup Onion.
 - Vendido como “O menor dispositivo Linux do mundo”
 - Combina o tamanho pequeno do Arduino com o poder e flexibilidade do Raspberry Pi
 - Usado em roteadores D-Link e outros dispositivos

Raspberry Pi e Onion



Protocolos de Comunicação



- MQTT: Message Queue Telemetry Transport - IBM
 - Simples, leve e de fácil implementação
 - Baixo consumo de bateria
 - Usado em redes com recursos limitados
 - Não foi pensado para segurança
 - Dados precisam ser criptografados em algum nível para garantir a segurança

Protocolos de Comunicação (II)



- CoAP: Constrained Application Protocol
 - Adaptação do protocolo HTTP para dispositivos com potência e capacidade de processamento limitados
 - Apresenta um conjunto mínimo de requisições (POST, GET, PUT, Delete) com suporte a armazenamento e descoberta de recursos
 - Usa protocolo DTLS para garantir a segurança
 - Utiliza menos recursos que HTTP normal
 - Envio de informações assíncronas – deixa dispositivo em sleep a maior parte do tempo

Protocolos de Comunicação (III)



- AMQP: Advanced Message Queuing Protocol
 - Padrão aberto de mensagens de middleware
 - Baseado em filas de mensagens orientadas a tópicos
 - Permite troca de mensagens por dispositivos com diferentes plataformas
 - Seguro: mensagens não podem ser reveladas ou alteradas por outros
 - Confiável: permite garantir a entrega da mensagem
 - Aberto e padronizado: especificação disponível para todos permitindo que diferentes implementações conversem entre si

Protocolos de Comunicação (IV)

- NFC: tecnologia para troca de informações entre equipamentos eletrônicos
 - Extensão do RFID
 - Permite a troca de informações dentro de uma distância máxima (alguns m)
- Wi-Fi – IEEE 802.11 (a, b, c, ac, n...)
- Zigbee: mais focada em ambiente industrial.
 - Baseado no padrão IEEE 802.15.4 – padrão para redes wireless industriais
 - Alcance de 10 a 100 m

Protocolos de Comunicação (V)



- Bluetooth: versão 5 se concentra em IoT
 - Baixo consumo de bateria
 - Alcance de até 240m

Problemas com os dados coletados



- Imperfeição
 - Imprecisão ou incerteza nas medidas coletadas
 - Causada por falha de hardware, falta de calibragem do sensor, mal posicionamento, etc
- Inconsistência:
 - Dados fora de sequência, presença de observações distantes das demais causadas por situações inesperadas ou dados conflitantes

Problemas com os dados coletados (II)



- Discrepâncias
 - Diferentes sensores capturam dados diferentes sobre um mesmo fenômeno

Segurança e Privacidade



- Segurança dos dados
- Segurança física pessoal e pública
 - Hackear carros e celulares
- Problemas de privacidade
 - Hackearam a câmera da empresa/ minha casa
- Problemas relacionados ao armazenamento e transmissão dos dados

Segurança e Privacidade (II)



- Confiabilidade: dados sensíveis não podem ser acessados por pessoas não autorizadas
- Integridade: os dados não podem ser alterados sem autorização enquanto estiverem armazenados no dispositivo ou durante a transmissão
- Tolerância a falha e monitoramento do status: garantir que falhas no dispositivo não levem a coleta de dados incorretos/atrasados
- Disponibilidade: o sistema deve estar sempre disponível

Mecanismos de segurança



- Criptografia dos dados
- Sistemas de autenticação robusta
- Hardware e software devem ser submetidos a testes de segurança
 - Invasão da rede
 - Ataque de negação de serviço [...]
- Dados sensíveis podem ser anonimizados para impedir que se saiba a quem se refere
- Manter software dos dispositivos atualizados
 - Correções de falhas de segurança

E o que vem depois?



- Ilot é para conseguir os dados
- Próximo passo é transformar esses dados em informações
 - Big Data
 - Machine Learning

Links



Bolsonaro institui o Plano Nacional de Internet das Coisas:

<https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/143072-bolsonaro-institui-plano-nacional-internet-coisas.htm>

Internet of Things Security Foundation - ESTABLISHING PRINCIPLES FOR
INTERNET OF THINGS SECURITY

<https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf>

Arduino <https://www.arduino.cc/>

Links



O Projeto de Firmware e de Hardware na IoT

<https://www.embarcados.com.br/o-projeto-de-firmware-e-de-hardware-na-iot/>

EXAMPLES OF INDUSTRY 4.0 USE CASES

<https://medium.com/@viarbox/examples-of-industry-4-0-use-cases-728938147570>

Exemplo: Fazenda

FUTURE FARMS small and smart

SURVEY DRONES

Aerial drones survey the fields, mapping weeds, yield and soil variation. This enables precise application of inputs, mapping spread of pernicious weed blackgrass could increase wheat yields by 2-5%.

FLEET OF AGRIBOTS

A herd of specialised agribots tend to crops, weeding, fertilising and harvesting. Robots capable of microdot application of fertiliser reduce fertiliser cost by 99.9%.

FARMING DATA

The farm generates vast quantities of rich and varied data. This is stored in the cloud. Data can be used as digital evidence reducing time spent completing grant applications or carrying out farm inspections saving on average £5,500 per farm per year.

TEXTING COWS

Sensors attached to livestock allowing monitoring of animal health and wellbeing. They can send texts to alert farmers when a cow goes into labour or develops infection increasing herd survival and increasing milk yields by 10%.

SMART TRACTORS

GPS controlled steering and optimised route planning reduces soil erosion, saving fuel costs by 10%.

