



IOT – INTERNET DAS COISAS

AULA 2



Prof. Gian Carlo Brustolin



CONVERSA INICIAL

Até aqui, quando conhecemos o conceito de IoT e as arquiteturas de objetos inteligentes, citamos exemplos de uso dessa tecnologia, em aplicações industriais, no agronegócio e em edificações comerciais ou residenciais. Nesta etapa, vamos conhecer, com certa profundidade, esta última aplicação, em edificações, cujo estudo e projeto recebe o nome de domótica.

Tradicionalmente, a domótica era focada em automação e controle de pequenas tarefas, baseadas em eletrônica embarcada, como iluminação e abertura de portas e portões em edificações residenciais. Neste estudo, veremos como os objetos e redes IoT se tornaram aplicáveis em projetos de automação residencial que evoluíram a domótica em direção à ideia da casa inteligente. Além da plena conectividade, a domótica passou a contar com soluções de cognição, bastante inovadoras, para uso residencial, simples e econômico (Stevan; Farinelli, 2018, p. 16).

Conheceremos, ainda, alguns objetos inteligentes, próprios para domótica e entenderemos de que forma placas para IoT podem automatizar utilidades domésticas, existentes comumente nos lares. Iniciaremos, também, o estudo sobre a conectividade para domótica, que certamente perturba a todos os usuários das facilidades propiciadas pela internet. Essa temática será objeto de aprofundamento posterior, em que, finalmente, compreenderemos como projetar e configurar corretamente um sistema WiFi residencial.

Peremptoriamente, analisaremos em conjunto as oportunidades de empreendedorismo, com o uso do conhecimento que adquirimos. Vamos, então, dar início nesse interessante estudo.

TEMA 1 – INTRODUÇÃO À DOMÓTICA

Com início artesanal, várias soluções para domótica são hoje produzidas em escala, permitindo a automação de boa parte das atividades domésticas. O envolvimento de IoT é recente, mas já há equipamentos de baixo custo disponíveis. O próximo passo, de inserção de inteligência, propiciado pelos objetos IoT e sua arquitetura IoT-A de processamento em nuvem, em breve popularizará as já existentes aplicações para casas inteligentes. Vamos entender como isso é possível.



1.1 Um pouco de história

A domótica tem uma história relativamente recente, ligada à popularização dos semicondutores na década de 1970. A partir daquele momento, a criação de artefatos eletrônicos se tornou economicamente viável, mesmo para projetos artesanais. Técnicos em eletrônica projetavam e produziam suas placas de circuito impresso, para automação de portões, interfones, câmeras de segurança, entre outros novos confortos e facilidades, para os lares daqueles que podiam contratá-los.

Por serem projetos únicos, a manutenção não poderia ser simples. Normalmente, o projetista se tornava, também, o mantenedor eterno da solução que a criou. O tempo selecionou os projetos mais comuns e estes foram incorporados à indústria.

Atualmente, em uma loja de departamentos, provavelmente encontraremos, disponível para aquisição imediata, mais de uma solução para a mesma facilidade de conforto ou segurança doméstica. Tomemos o exemplo de portaria eletrônica, equipamentos produzidos em série, que agregam facilidades, como comunicação por voz, imagem, controle de fechadura, acionamento de portões e, em boa parte dos casos, permitem o acesso remoto, pela internet.

Essa disseminação passou a demandar o desenvolvimento de acionadores e sensores que compartilham parte de sua arquitetura com dispositivos utilizados em automação industrial. Embora ainda em estágio inicial, a ideia de importar as soluções utilizadas nas modernas redes interoperáveis de sensores e atuadores industriais é uma tendência irreversível.

Dotar os objetos de capacidade de conexão com protocolos genéricos de rede exige embarcar certa inteligência nesses dispositivos. Presente a inteligência, mais usos dela é possível extrair. Dessa forma, a ideia da casa inteligente se vê viabilizada.

1.2 IoT-A para domótica

Aplicações residenciais precisam ser extremamente fáceis de usar e configurar, pela óptica do usuário, naturalmente. Como a apresentado na ilustração a seguir, o usuário busca objetos autoconfiguráveis e que, interconectados com a internet, ou rede interna, permitem controle simples e homogêneo.



Figura 1 – Objetos autoconfiguráveis para domótica



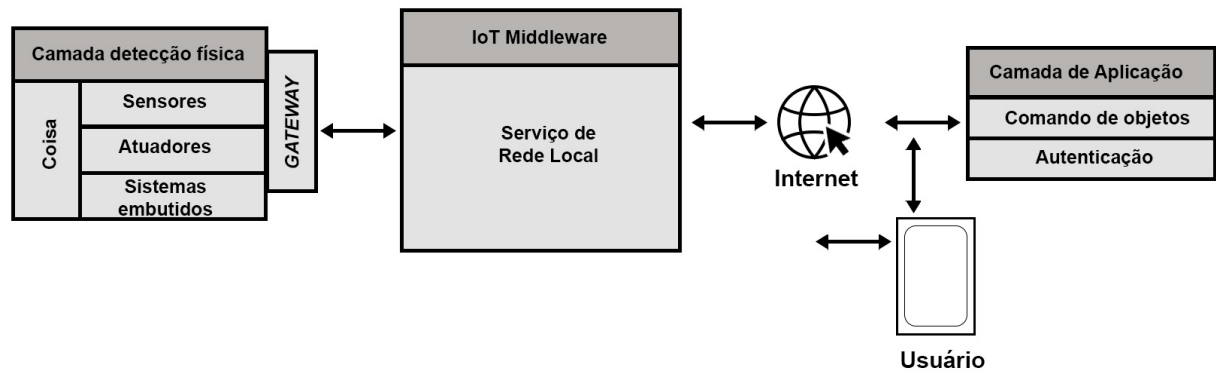
Crédito: stockwerk-fotodesign/Shutterstock.

Arquiteturas de baixo nível, que demandam programações complexas, são um bom desafio de engenharia, mas não são aplicáveis em domótica, sob o risco de retrocedermos aos antigos projetos dedicados, de difícil manutenção e sem escalabilidade.

A escolha por uma IoT-A, de alto nível, é natural; dessa forma, a arquitetura de três camadas é sempre escolhida para aplicações em domótica. Prédios inteligentes, principalmente comerciais, podem admitir arquiteturas com quatro camadas. Nesses casos, abre-se mão das facilidades de autoconfiguração em prol de sensores/atuadores mais baratos, que demandarão complementos externos para sua capacidade de conexão e processamento.

O detalhamento da IoT-A de três camadas está presente em nossa discussão inicial, vamos apenas relembrar seu desenho (figura a seguir), de forma esquemática e adaptada à aplicação em domótica.

Figura 2 – IoT-A de três camadas para domótica



Crédito: Maschietto *et al.*, 2021, p. 62.

Como é possível observar, os objetos estão conectados autonomamente à rede local. Normalmente, essa conexão é sem fio e se dá via WiFi.

A rede local se encarregará da distribuição de endereço, controle de acesso e, ao menos teoricamente, segurança. A inteligência de sensoriamento/atuação estará residente no objeto. Na internet, teremos uma aplicação com a função de comandar os objetos, seguindo o controle do usuário. A mesma aplicação de nuvem realizará a autenticação dos usuários autorizados.

Essa aplicação de nuvem pode ser desenvolvida por uma empresa prestadora de serviços, que se responsabilizará por sua manutenção e associará seu fornecimento a outros tipos de facilidades, como reabastecimento de gás, segurança patrimonial, manutenção de equipamentos etc.

Aplicações de nuvem gratuitas também existem, fornecidas pelos fabricantes dos objetos, ou de companhias de internet, como *Amazon* e *Google*, mas esse assunto estudaremos posteriormente.

Para o usuário, essa topologia é transparente. O acionamento dos objetos se dá de forma similar a um controle remoto local, o que, de fato, está bastante distante da realidade de rede, como acabamos de estudar.

Nesse ponto, você seguramente está curioso quanto às aplicações e controles possíveis. Vamos, então, mergulhar, nos próximos tópicos, nos objetos existentes (próprios e impróprios), na conectividade deles e nas aplicações de nuvem gratuitas.

TEMA 2 – OBJETOS IoT PARA DOMÓTICA

Conhecemos dois tipos de objetos IoT, classificados segundo seu projeto. Há aqueles que possuem inteligência e conectividade nativas, aos quais denominamos próprios e outros que necessitam acréscimo de eletrônica



(impróprios). Aqui, vamos conhecer alguns desses objetos e como é possível acrescentar inteligência e controle a uma eletrônica preexistente.

2.1 Objetos próprios para domótica

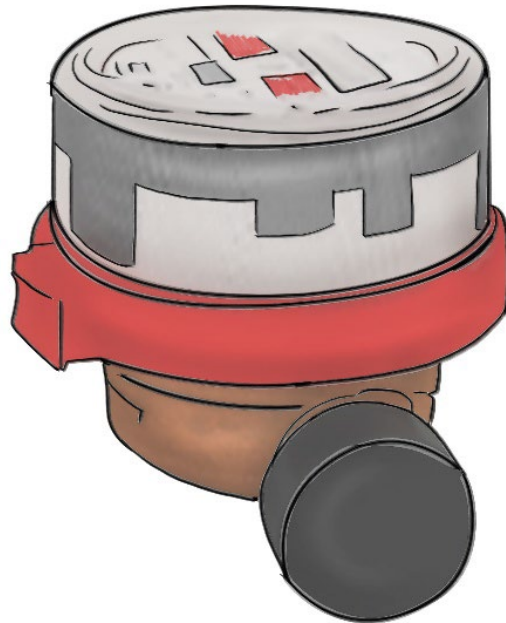
Quando fizemos nossa breve revisão histórica da domótica, afirmamos que já existem, comercialmente disponíveis, objetos inteligentes de baixo custo, para uso em domótica. De fato, a criação de objetos IoT, próprios para domótica, pode ser encarada como uma particularidade dos impróprios, cuja aplicação de larga escala tornou a produção de circuitos eletrônicos dedicados, contendo todos os blocos funcionais, economicamente viáveis.

Há objetos próprios, que estão suficientemente popularizados, para que possamos falar deles, sem surpresa alguma. Câmeras de vídeo, caixas de som e sensores de porta, por exemplo, são dispositivos que podem operar como objetos IoT, disponíveis em lojas de departamentos.

Existem, entretanto, alguns objetos menos conhecidos, como sensores de CO₂, detectores de metano e sensores de nível de água, com conectividade nativa para WiFi, ou outras redes para IoT.

A seguir ilustramos um sensor de nível de água com conectividade LoRa. Como veremos, a seleção dessa interface, embora apresente dificuldades de interconexão direta com rede WiFi padrão TCP, permite a operação sem alimentação externa, com uso de baterias pequenas, por vários anos sem necessidade de troca. Essa pode ser uma vantagem interessante para instalação em locais de difícil acesso e sem rede elétrica disponível.

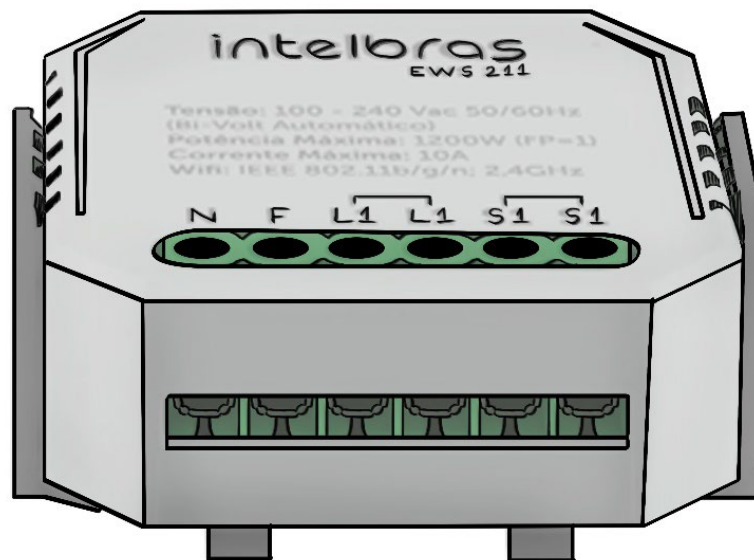
Figura 3 – Sensor de nível com interface LoRa



Crédito: Jefferson Schnaider.

Esses objetos, não muito conhecidos, podem ter uma utilidade considerável, no incremento da segurança residencial. Com o uso de detectores de metano, por exemplo, podemos evitar a explosão de ambientes em consequência de vazamento de gás de cozinha. Sensores de CO2 podem evitar o sufocamento de bebês, ou mesmo ligar a ventilação, em caso de excesso de CO2 em dado ambiente. Aliás, para realizar o acionamento de um equipamento simples, como um exaustor ou da iluminação, há interruptores IoT (veja figura a seguir) que se conectam diretamente ao WiFi e permitem a operação desses equipamentos, diretamente por um aplicativo de nuvem.

Figura 4 – Interruptor de energia inteligente



Crédito: Jefferson Schnaider.

Há vários objetos que atendem, praticamente, a todas as necessidades de automação residencial. Uma pesquisa na internet é suficiente para localizar uma miríade de dispositivos. Encontrar, instalar e integrar esses objetos pode ser, inclusive, uma boa oportunidade de negócios, tópico que discutiremos ainda nesta etapa.

Talvez, depois de pensar sobre os objetos IoT, você pode estar imaginando como integrar a essa rede objetos domésticos, que não têm conectividade nativa, como máquinas de lavar e sistemas de aquecimento. Esses são os objetos que podem receber placas de adaptação, objetos IoT impróprios. Vamos tratar deles a seguir.

2.2 Objetos impróprios para domótica

Ao introduzirmos o tópico, dissemos que máquinas domésticas, como lavadoras, aquecedores e condicionadores de ar, sem conectividade nativa à internet, podem ter uma eletrônica agregada que possibilite sua transformação em objetos IoT inteligentes. A mágica por trás disso são as placas para IoT.

Para entendermos essas placas, devemos voltar ao nosso estudo da arquitetura interna de um objeto inteligente. Naquele momento dividimos o dispositivo em blocos: identificação, comunicação, processamento, semântica, serviços e sensores.

Máquinas domésticas, como as que citamos anteriormente, são dotadas de uma eletrônica embarcada, que permite seu controle local, pelo humano. Dessa forma, são dotadas dos últimos dois blocos funcionais (serviços e



sensores) e algum processamento, a fim de tornar a interface homem-máquina possível. O que se pretende é agregar a essas máquinas ao menos os três primeiros blocos, da arquitetura interna dos objetos IoT.

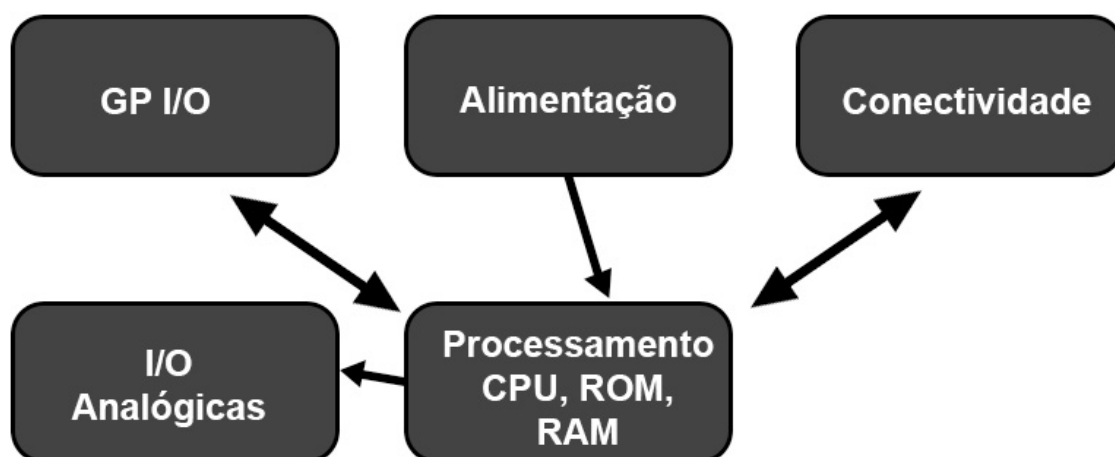
Por isso, uma placa para IoT deverá conter, minimamente, um processador capaz de controlar a eletrônica legada e uma interface de comunicação, com a rede TCP doméstica, preferencialmente sem fio. Essa preferência, no caso das aplicações em domótica, é importante para que se evite transformar a residência em um emaranhado de cabos de rede, que certamente desagradaria esteticamente a seus habitantes. Usamos o termo “preferência” porque existirão objetos que demandarão conexão fiada; sobre essa discussão, voltaremos em tópico próximo sobre conectividade.

Assim como objetos IoT são produzidos industrialmente e podemos comprá-los na internet, ou em uma grande loja, placas para IoT também o são.

Seguindo a mesma estratégia pedagógica utilizada para descrever os objetos, vamos apresentar uma placa para IoT, genérica, pela sua divisão em blocos funcionais.

Os blocos de uma placa para IoT, como mostrados na figura seguinte, podem ser sintetizados nas funções de processamento, I/O (analógicas e GP), alimentação e conectividade.

Figura 5 – Blocos rudimentares da placa de IoT



Crédito: Brustolin, 2022.

O **processamento** de uma placa IoT é composto por um chip de CPU, normalmente com memórias integradas. Como em uma máquina computacional tradicional, esse bloco executará a aplicação residente na ROM (firmware), controlando a placa, a eletrônica legada e a conectividade com a rede.



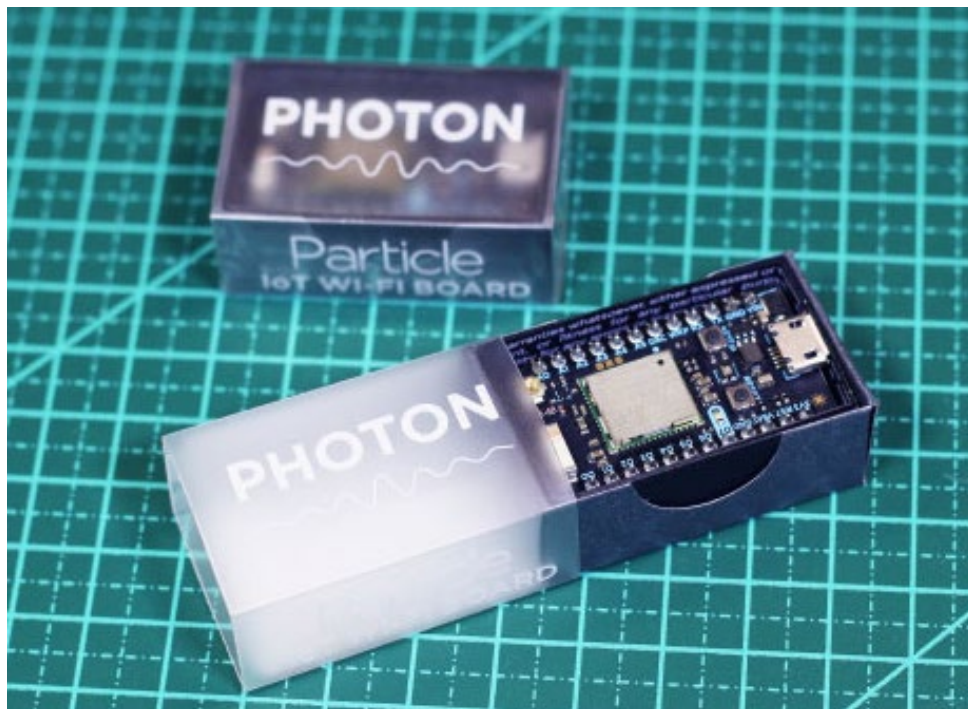
Há dois blocos de **I/O** (In/Out ou entradas e saídas), uma vez que a placa possui interfaces digitais (um exemplo é a interface USB normalmente presente em placas de IoT), dita de “propósito geral” (GP – *general purpose*, em inglês) e analógicas. As I/Os analógicas permitem a conexão direta a sensores e atuadores, sem a necessidade de converter níveis de tensão em dados binários.

A **alimentação** de uma placa para IoT dificilmente é feita pela rede elétrica diretamente, PoLP ou a própria interface USB, são o uso comum. Uma observação interessante refere-se à capacidade de adormecimento de algumas dessas placas, que permitem o uso de baterias ou pilhas sem substituição por anos.

A **conectividade** das placas para IoT objetiva a troca de dados com redes TCP e se dá, predominantemente, pela interface rádio padrão 802.1x, mas como já dissemos, voltaremos ao tópico de conectividade em breve, dispensando a discussão por ora.

A eletrônica de uma placa para IoT precisa ser bastante compacta, econômica e flexível, para permitir seu uso nas aplicações de domótica. Para que possamos tomar contato com essas eletrônicas, a figura seguinte apresenta uma placa IoT *Photon*, cujas dimensões se aproximam de uma caixa de fósforos.

Figura 6 – Placa *Photon* para IoT

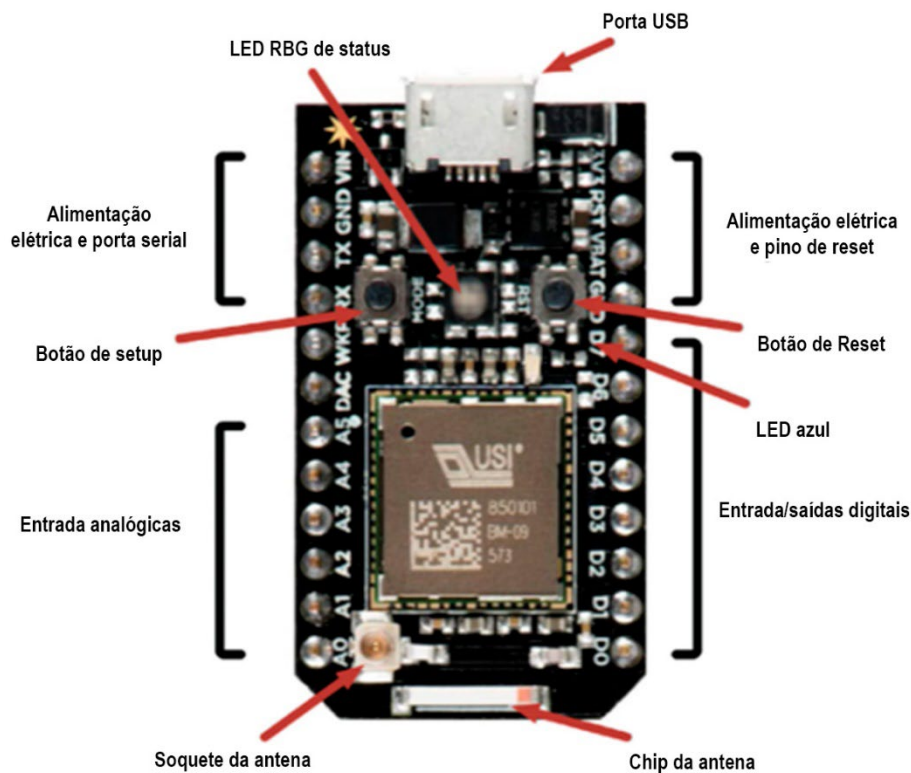


Disponível em: <<https://www.filipeflop.com/blog/projetos-iot-com-a-particle-photon/>>. Acesso em: 3 out. 2022.



A próxima figura amplia a placa, para que possamos identificar os blocos funcionais, citados anteriormente.

Figura 7 – Placa *Photon* para IoT



Crédito: Monk, 2018.

Uma placa para IoT, por ter propósito geral, além do estudo de conexão eletrônica, precisa ser programada para operar uma máquina residencial. Apenas por curiosidade, vamos conhecer como essa programação é feita.

2.3 Programação de placas para IoT

Aqui, não temos por objetivo aprofundar os estudos sobre programação de placas IoT. Apenas forneceremos algumas noções, que serão importantes, caso se necessite criar aplicação, que integre as placas com outros objetos IoT.

Quando objetivamos programar uma placa para IoT, desejamos, de fato, programar o processador presente na placa. Você deve estar pensando que estamos para mergulhar em um daqueles abismos de programação de baixíssimo nível, já que as placas são muito rudimentares. Essa conclusão está, apenas, parcialmente correta.



De fato, toda máquina computacional, mesmo o computador ou celular que você está, eventualmente, usando para ler esta etapa agora, quando ligado, executa um programa de inicialização, *firmware*, que configura o ambiente básico do usuário. Sobre esse ambiente, será instalado o sistema operacional e as demais aplicações sobre este último.

A programação de um processador parte desse setup de *firmware*, cujos comandos são o próprio conjunto de instruções do processador. Mas, calma, mesmo nesse baixíssimo nível, há IDEs (*Integrated Development Environments*) para auxiliar na codificação em mais alto nível. Precisamos entender, portanto, que nosso código, para residir na memória não volátil da placa, precisa ser compilado gerando, inicialmente, o microcódigo (em *Assembly*). O microcódigo passará um por assembler que o converterá em *opcode* hexadecimal. No momento de gravação na memória, o *opcode* será reduzido para binário e, finalmente, gravado!

Naturalmente, a IDE gerencia esse processo e não é necessário, para o humano, descer ao binário para realizar a tarefa. Por outro lado, é fato que o uso de IDEs, com linguagens de alto nível, geram códigos de baixa eficiência e alto uso de memória. Esses são dois fatores a serem evitados em placas para IoT, em que há francas limitações de espaço de armazenamento e capacidade de processamento (Lenz; Torres, 2019, p. 96). Isso quer dizer que, se você precisar desenvolver uma interface para essas placas, precisará ter conhecimento de linguagens mais próximas ao Assembly, como o C, por exemplo.

TEMA 3 – CONECTIVIDADE IOT PARA DOMÓTICA

Em nossa introdução, comentamos que a conectividade dos objetos IoT, sejam objetos próprios ou não, é um tema tão importante quanto o próprio objeto. Teremos, durante nosso estudo, um momento específico para o estudo de soluções de rede para IoT. Neste tópico, trataremos especificamente da interconexão de objetos por rede WiFi. A escolha do padrão WiFi se dá pela franca liderança dessa tecnologia em aplicações residenciais, frente a todas as demais soluções (Tic Domicilios, 2021). Há um outro padrão relativamente comum, dito ZigBee, usado como alternativa para conexão de objetos *stand alone*, quando o consumo de energia dos objetos é um fator imprescindível para o sucesso do projeto. Esse padrão não será detalhado aqui, mas reservaremos para ele um breve estudo ainda neste curso.



As questões de segurança são uma discussão a parte, principalmente em domótica. A exposição de objetos IoT, de automação residencial, na internet, pode ter consequências mais danosas que aquelas para redes que não possuam tais objetos. Trataremos deste tópico de segurança, com detalhes em outro momento, mas não há cuidado excessivo ao se projetar uma rede sem fio para esse fim, já que os riscos são consideráveis.

3.1 Introdução ao padrão 802.11 e suas versões

Redes de objetos IoT com conectividade WiFi são bastante comuns e o uso desse protocolo para IoT não difere dos projetos de redes locais. Dessa maneira, o que abordaremos a seguir se aplica a redes locais sem fio. As redes sem fio (WLAN – *Wireless LAN*) WiFi foram padronizadas pelo Instituto de Engenheiros Elétricos e Eletrônicos (IEEE) no final do século passado.

No que se refere às versões, a primeira produzida em série foi a 802.11b, seguida pelo IEEE802.11a, 802.11 g e **IEEE 802.11n** (que recebeu o apelido de **WiFi 4**). Esta última versão, com boa velocidade de transmissão, resiliência de conexão e custo baixo, sacramentou o uso de WiFi como método de acesso preferencial em redes TCP. O WiFi 4, entretanto, não era perfeito, os problemas surgiram quando a densidade de usuários das redes começou a subir. Foi necessário, então, contornar o problema de densidade de usuários. A ideia foi utilizar a solução já sedimentada nas gerações mais recentes de telefonia celular, adaptando o *Multiple-Input Multiple-Output* (Mimo), que passou a fazer parte das versões seguintes.

A primeira versão a utilizar essa técnica, produzida em 2018, foi o **IEEE 802.11ac**, batizado de **WiFi 5**. Este ainda é o mais popular em uso corporativo, enquanto a maioria das implantações residenciais permanece com a versão 4.

O WiFi 5 permite a transmissão de até 400 Mbps, em 2,4GHz e até 7Gbps em SHF (em condições ideais de propagação). Nessa versão, os problemas de densidade foram resolvidos, mas como as condições ideais de propagação nunca ocorreram, de fato, o padrão dificilmente atinge a velocidade prometida.

A observação do comportamento efetivo das colisões de rede deu origem a um novo padrão, **IEEE 802.11 ax**, ou **WiFi 6**, que ainda aguarda uma utilização extensiva. Novas versões de normas já estão disponíveis no IEEE, mas ainda não há produtos no mercado que as embarque em número perceptível.



Em todas as versões (a exceção da versão 802.11 ah, dita *HaLow*, bastante recente e de aplicação específica), o IEEE manteve o foco em alto desempenho, baixo custo e alta densidade de usuários com alta demanda de dados. Dessa forma, o uso de WiFi para objetos IoT presume que há disponibilidade para alimentação desses dispositivos. **Dispositivos que precisam utilizar baterias próprias, de alta duração, não podem ser atendidos por WiFi.** Esse fato, entretanto, não invalida a grande quantidade de objetos inteligentes, sem essa restrição, que podem ser conectados com o uso dessa interface.

3.2 Conexão de objeto IoT ao WiFi

Um objeto IoT, ao ser energizado, inicialmente entra em modo de configuração. Nesse modo, o rádio interno do dispositivo comporta-se como um ponto de acesso (AP), gerando uma rede com identificação (SSID) própria. O instalador então conecta-se a esse AP temporário e fornece as informações de identificação e senha da WLAN na qual deseja instalá-lo. Em seguida, o objeto é reiniciado e se loga no AP da rede local.

Podemos, então, localizá-lo na rede local e habilitar sua operação pelo aplicativo de nuvem que controla os objetos da rede.

Muitos fabricantes de objetos têm sites que simplificam o processo de configuração. Os objetos, após receberem as informações da rede local, ganham acesso à internet e se logam automaticamente nesses sites. Aqui reside um dos principais problemas de segurança no uso desses objetos, ao pré-configurar o objeto, deixamos a rede local acessível para à internet. A segurança é de vital importância, mas trataremos dela em outro momento.

3.3 Introdução ao padrão IEE 802.15.4g (ZigBee)

A conectividade WiFi foi criada pelo IEEE com foco em desempenho e baixo custo. Essas interfaces, guardado o que comentamos anteriormente, têm baixa preocupação com o consumo de energia do rádio e do processamento associado.

O padrão ZigBee teve origem na tentativa de atender a redes de sensoriamento (WSN – *Wireless Sensor Network*) para aplicação industrial, com foco em redução de custos, baixo consumo de energia, baixa taxa de falhas e fáceis de se manterem. Essas características tornaram, recentemente, ZigBee



uma opção para o agronegócio, para aplicação em agricultura de precisão, por exemplo.

Objetos inteligentes para domótica podem ter demandas semelhantes, quando são instalados em locais de difícil acesso para a rede elétrica. Limites de propriedade, caixas d'água, topos de árvores, são exemplos de locais que demandam objetos *stand alone*.

O protocolo das camadas superiores do ZigBee não é compatível com o padrão TCP, exigindo a presença de um *gateway* de interfaceamento. Se você ficou curioso sobre os detalhes desse protocolo, acesse a documentação presente em Zigbee, 2020, referenciada nas fontes de pesquisa desta etapa.

TEMA 4 – CAMADA DE APLICAÇÃO E CONTROLE

Quando descrevemos a IoT-A de um objeto para domótica, apresentamos a Figura 2, como diagrama esquemático de conexão. Fomos, naquele momento, propositalmente simplistas. Neste tópico, aprofundaremos nosso conhecimento sobre a camada de aplicação e controle, típica para objetos IoT, aplicados em domótica.

A escolha de um objeto para domótica está normalmente vinculada à sua compatibilidade com um “assistente pessoal”, com um *gateway* ou com uma nuvem corporativa, a exemplo da *Google Home*. Vamos agora entender o papel de cada um desses elementos.

4.1 Solução de nuvem

Há vários objetos IoT para aplicação em automação residencial que são compatíveis com o protocolo IP e rádio 802.11. Os fabricantes de tais objetos normalmente seguem o padrão de configuração, que comentamos no tópico anterior e que disponibilizam integração com algumas aplicações de nuvem de grandes corporações como *Amazon* e *Google*. Essas aplicações podem auxiliar na configuração do objeto e, posteriormente, permitem seu controle integrado com os demais objetos.

A nuvem da *Google*, por exemplo, pode ser controlada diretamente por um dispositivo móvel. Alternativamente, há também assistentes pessoais, comercializados por parceiros da empresa, que permitem o controle de forma mais amigável. Um exemplo desse modelo de controle, com uso de assistente pessoal, é o *hardware Echo* comercializado pela *Amazon*. O dispositivo pode



controlar objetos IoT, além de realizar tarefas de assistência, como busca na internet por comando de voz, reprodução de músicas etc. O *Echo* também possui uma IA associada (*Alexa*).

A configuração de um *Echo* é relativamente simples, mas necessita da conexão ao site da *Amazon*. O usuário, com o aplicativo *Alexa* em seu *smartphone*, é capaz de personalizar o *Echo* e acrescentar dispositivos, conforme ilustrado a seguir. A configuração é concluída com o uso combinado do *Bluetooth* do *smartphone*. Esse recurso evita as buscas por endereços IP e configurações de rede, necessárias no caso de outras soluções que veremos posteriormente.

Figura 8 – Aplicação de nuvem *Amazon Alexa*



Disponível em: <<https://gizmodo.uol.com.br/alexa-smartphone-nova-tela-inicial-escutar-comandos/>>. Acesso em: 3 out. 2022.

A configuração de dispositivos segue o mesmo procedimento. Será necessário adquirir objetos compatíveis com a IA da *Amazon*, mas cumprida essa restrição, todas as informações necessárias à integração estão disponíveis no servidor da empresa.

4.2 Controle por HW

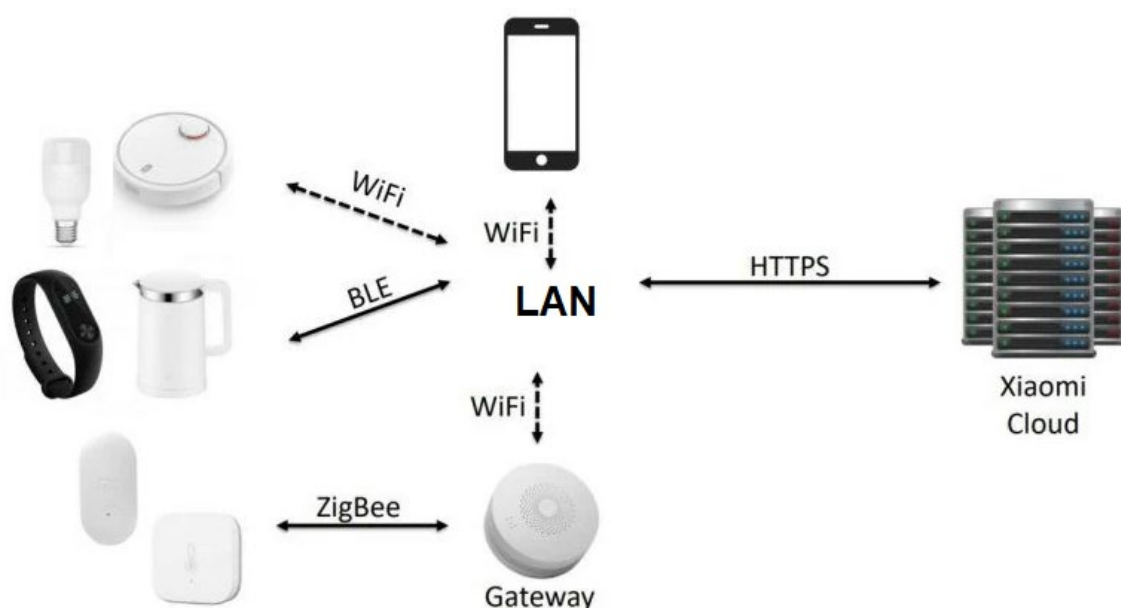


Para que um objeto seja controlável em nuvem, conforme já afirmamos, seu *firmware* deve ser compatível com as aplicações de nuvem. E se não for? Há uma segunda solução possível de controle, o uso de um *hardware* conectado à LAN, dito *gateway* IoT. Os *gateways* podem também receber a designação genérica, leiga, de *hubs* inteligentes ou assistentes pessoais. Do ponto de vista técnico, um assistente pessoal não é um *gateway*, uma vez que não realiza a conversão de interfaces. Dessa forma, devemos usar a designação *gateway* para o *hardware* que realizará a interface entre o controle de nuvem ou, no contexto da rede local, por aplicativo de alto nível, móvel ou não.

O *gateway* de IoT, para domótica, se conectará com os objetos inteligentes da residência pelo protocolo IP, da rede local ou por outros protocolos de comunicação, suportando a interface entre o aplicativo de comando do usuário e esses objetos. Existe uma boa quantidade de *gateways* disponíveis no mercado. Comentaremos brevemente sobre um modelo, para que tenhamos exemplo concreto do que já comentamos.

O *gateway* *Aqara*, produzido pelo fabricante chinês Xiaomi integra uma boa quantidade de objetos ZigBee e WiFi. A configuração desse *gateway* depende do acesso a um servidor, mantido pelo fabricante, que contém os pacotes para cada objeto. O diagrama de conexão é apresentado na figura a seguir. Como já sabemos, o padrão ZigBee, interface rádio padronizada pela norma IEEE802.15.4, suporta conexão a objetos com menor demanda de energia, em relação ao WiFi, e maior resiliência de conexão.

Figura 9 – Arquitetura de conexão de objetos IoT e *gateway* *Aqara*





Disponível em: <<https://pt.xiaomitoday.it/xiaomi-possui-500-milh%C3%B5es-de-usu%C3%A1rios-ativos-em-todo-o-mundo.html>>. Acesso em: 3 out. 2022.

Dispositivos gerenciáveis pelo *Aqara*, com interface rádio ZigBee, podem permanecer sem troca de bateria por até 2,5 anos.

Concluída a configuração, será necessário utilizar um aplicativo de controle do *gateway*. O aplicativo disponibilizado pela Xiaomi é bastante rudimentar, mas há informações nos sites do fabricante que permitem o desenvolvimento de aplicativo dedicado.

A Xiaomi, recentemente, buscando uma solução mais simples para o usuário, integrou o *hub* com o assistente da *Apple*, *Home Kit*, associado com a IA de assistência, Siri. Outras integrações estão disponíveis, inclusive com a *Alexa* da *Amazon*, mas, nesses casos, ao menos até este momento, é necessário configurar os objetos no *gateway* e, posteriormente, integrá-lo a IA.

TEMA 5 – EMPREENDEDORISMO EM DOMÓTICA COM IoT

Aqui, vamos entender algumas oportunidades de negócio ligadas ao IoT e especialmente relacionadas à sua aplicação em Domótica. Não pretendemos elaborar um rol taxativo de negócios na área, mesmo porque a própria IoT é uma tecnologia ainda adolescente e sofrerá constantes e profundas modificações nos próximos anos.

5.1 IoT e mercado de consumo

Se, por um lado, pairam dúvidas sobre o caminho de que a evolução da IoT, por outro não há questionamento sobre sua presença crescente nos ambientes industriais, comerciais, públicos e residenciais. Uma boa leitura, para aprofundar este assunto dos usos e tendências, está em Magrani (2018).

Como forma de exemplificar a significativa compleição dessa tecnologia, para o comércio, tomemos a questão da satisfação de clientes. Tentar satisfazê-los, em grandes corporações comerciais, já não é uma vantagem comercial, mas uma questão de sobrevivência.

Empresas que não possuem sistemas eficientes de avaliação e atuação na satisfação de clientes perdem participação de mercado, paulatinamente. Prova disso são os sistemas de CRM (*Customer Relationship Management*), antes tecnologia inovadora, fazem agora parte da coleção de SWs essenciais à



administração dos negócios, permitindo gerenciar custos de aquisição de novos clientes, retenção e manutenção dos clientes conquistados (Lima, 2018, p. 87).

Um diferencial na estratégia de CRM é a resposta rápida aos desejos e problemas dos clientes. As tentativas, nesse sentido, utilizam, tradicionalmente, estudos baseados em pesquisas de satisfação e opinião. Mais recentemente aproximações baseadas em *big data* e IA aceleram a extração de dados e tornam as conclusões praticamente instantâneas. O processo, entretanto, é ainda reativo, baseado em dados passados.

Tecnologias IoT, voltadas ao consumo, podem ser o ponto de inflexão dessa forma de avaliação de dados para tomada de decisão. Objetos IoT podem ser habilitados a avaliar necessidades pessoais antes que se tornem impulsos de compra. Podemos encontrar exemplos de aplicação em saúde, manutenção de veículos, conservação de prédios etc.

O uso de objetos IoT para esse tipo de aplicação, de predição de consumo, não apenas beneficia as corporações, mas pode ter impacto positivo na segurança pessoal, preservação do meio ambiente e qualidade dos produtos.

Certamente, aqui, há várias oportunidades de empreender, dado o estágio inicial de desenvolvimento da tecnologia.

5.2 Go to Market

Modelos de negócio tradicionais pouco podem ensinar para o “Go to Market” de um produto IoT. O fato de se tratar de uma tecnologia ainda em estágio inicial faz com que as possíveis aplicações sejam praticamente infinitas, mas, pragmaticamente, poucas são implementáveis em curto espaço de tempo. Deve-se esperar uma boa dose de pesquisa e desenvolvimento para que as soluções se tornem parte da cadeia de decisão de uma organização ou do dia a dia de um cliente.

Dessa forma, apesar do baixo custo unitário e facilidade de implementação dos objetos, não se pode esperar que o desenvolvimento de um produto baseado em IoT tenha essas mesmas características. Estratégias de rápido compartilhamento do custo de desenvolvimento precisam ser estudadas para viabilizar os projetos.

Um bom caminho é acompanhar a tendência da economia compartilhada, a exemplo de serviços como Uber, AirBnB, Waze, que permitem a disseminação rápida e em escala. Outro aspecto, que pode servir de facilitador na remuneração



desses custos é a agregação de IA aos dados coletados pelos objetos inteligentes de forma a avaliar, de forma preditiva, a experiência do usuário (Magrani, 2018, p. 131 e seguintes).

5.3 Domótica

As aplicações de objetos IoT em domótica, como pudemos observar no decorrer de toda a etapa, são múltiplas, de bom custo-benefício e fácil implantação. Dessa forma, o que sustentamos anteriormente, sobre os problemas de modelagem de negócio, já estão relativamente superados nas aplicações residenciais. Boa parte dos objetos úteis para automação residencial já se encontram disponíveis e são integráveis às aplicações de nuvem.

A criação de um negócio com foco em IoT, para domótica, tem poucas barreiras de entrada, a exceção do conhecimento técnico, que pode ser por nós adquirida, com esforço reduzido em relação à população leiga.

Qualquer empreendimento apresenta, naturalmente, alto risco e a simples vantagem competitiva ligada ao conhecimento não é fator determinante do sucesso. Planos de negócio precisam ser estruturados e associados a pesquisa de mercado e demanda. Não há dúvidas que essa aplicação é um campo arável e ainda pouco explorado, mas há necessidade de substancial apoio mercadológico para qualquer iniciativa empreendedora.

FINALIZANDO

Nesta etapa, entendemos como objetos IoT podem ser aplicados em prédios e residências. Estudamos as arquiteturas, interna e externa, necessárias para essa aplicação, bem como sua solução mais frequente de conectividade. Entendemos a necessidade de conexão à internet e consideramos os riscos à segurança, provenientes dessa necessária exposição, deixando sua análise e tratamento para outra ocasião.

Em outro momento, ampliaremos substancialmente nossa visão sobre a aplicação dos objetos IoT, discutiremos tecnologias emergentes de IoT em *smart cities*, tópico empolgante e extremamente interessante para nosso futuro como profissionais de tecnologia.



REFERÊNCIAS

MASCHIETTO, L. *et al.* **Arquitetura e Infraestrutura de IoT**. Disponível em: Minha Biblioteca, Grupo A, 2021. MB.

LENZ, M.; TORRES, F. E. **Microprocessadores**. Disponível em: Minha Biblioteca, Grupo A, 2019. (MB).

LIMA, A. W. B. *et al.* **Indústria 4.0: Conceitos e Fundamentos**. São Paulo: Blucher, 2018.

MAGRANI, E. **Internet das coisas**. Online. Rio de Janeiro: FGV Editora, 2018. Disponível em: <<https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y>>. Acesso em: 13 maio 2020.

MONK, S. **Internet das Coisas**: uma Introdução com o Photon – Série Tekne Grupo A, 2018. ISBN 9788582604793. MB.

STEVAN Jr, S. L.; FARINELLI, F. A. Domótica - automação residencial e casas inteligentes com Arduino e ESP826. Disponível em: Minha Biblioteca, Editora Saraiva, 2018.

TIC DOMICILIOS 2021. **Pesquisa do CETIC BR**. Disponível em: <https://www.cetic.br/media/analises/tic_domicilios_2021_coletiva_imprensa.pdf>. Acesso em: 30 set. 2022.

ZIGBEE. **Developer Resources Papers**. Disponível em: <https://zigbeealliance.org/developer_resources/?solution_type%5B%5D=zigbee>. Acesso em: 5 jun. 2020.