Universidade do Sul de Santa Catarina

Pós-Graduação

Internet das Coisas

Autor
Mauro Faccioni Filho

UnisulVirtual

Créditos

Universidade do Sul de Santa Catarina – Unisul

Reitor
Sebastião Salésio Herdt
Vice-Reitor
Mauri Luiz Heerdt

Pró-Reitor de Ensino, de Pesquisa e de Extensão
Mauri Luiz Heerdt
Pró-Reitor de Desenvolvimento Institucional
Luciano Rodrigues Marcelino
Pró-Reitor de Operações e Serviços Acadêmicos
Valter Alves Schmitz Neto

Diretor do Campus Universitário de Tubarão
Heitor Wensing Júnior
Diretor do Campus Universitário da Grande Florianópolis
Hércules Nunes de Araújo
Diretor do Campus Universitário UnisulVirtual
Fabiano Ceretta

Campus Universitário UnisulVirtual

Diretor
Fabiano Ceretta

Unidade de Articulação Acadêmica (UnA) – Ciências Sociais, Direito, Negócios e Serviços
Amanda Pizzolo *(coordenadora)*
Unidade de Articulação Acadêmica (UnA) – Educação, Humanidades e Artes
Felipe Felisbino *(coordenador)*
Unidade de Articulação Acadêmica (UnA) – Produção, Construção e Agroindústria
Anelise Leal Vieira Cubas *(coordenadora)*
Unidade de Articulação Acadêmica (UnA) – Saúde e Bem-estar Social
Aureo dos Santos *(coordenador)*

Gerente de Operações e Serviços Acadêmicos
Moacir Heerdt
Gerente de Ensino, Pesquisa e Extensão
Roberto Iunskovski
Gerente de Desenho, Desenvolvimento e Produção de Recursos Didáticos
Márcia Loch
Gerente de Prospecção Mercadológica
Eliza Bianchini Dallanhol

Mauro Faccioni Filho

Internet das Coisas

Livro Digital

Designer instrucional
Marina Cabeda Egger Moellwald

UnisulVirtual
Palhoça, 2016

Livro Digital

Professor conteudista
Mauro Faccioni Filho

Designer instrucional
Marina Cabeda Egger Moellwald

Projeto gráfico e capa
Equipe UnisulVirtual

Diagramador(a)
Pedro Teixeira

Revisora
Diane Dal Mago

F12

Faccioni Filho, Mauro

Internet das coisas : livro digital / Mauro Faccioni Filho ; design instrucional Marina Cabeda Egger Moellwald. – Palhoça : UnisulVirtual, 2016.

56 p. : il. ; 28 cm.

Inclui bibliografia.

Internet (Rede de computadores). 2. World Wide Web (Sistema de recuperação da informação). I. Moellwald, Marina Cabeda Egger. II. Título.

CDD (21. ed.) 004.678

Ficha catalográfica elaborada pela Biblioteca Universitária da Unisul

Sumário

Apresentação

A internet é algo que está em nossas vidas há apenas duas décadas, e já é essencial para nossos negócios, lazer e relações sociais. Integrou praticamente todos os processos comerciais e empresariais, e sem a internet já não é possível trabalhar ou mesmo pagar contas. No entanto, uma nova revolução está em curso, e seu nome é “Internet das Coisas”.

Inicialmente, a internet era uma rede de computadores com conectividade mundial. Partiu da conexão entre universidades, governos, órgão militares e, depois, entrou no ambiente comercial e em nossas vidas privadas. Mas sempre baseada em redes de computadores, que aos poucos incluiu tablets e celulares, sendo que, atualmente, os celulares já ultrapassam os computadores em acesso à internet. Esse avanço dos celulares, a miniaturização eletrônica, e diversos outros processos que utilizam equipamentos minúsculos e que dispõem de processamento e capacidade de comunicação em rede deram origem a uma nova realidade, que foi batizada de internet das coisas, ou seja, de objetos ou “coisas” que conseguem se comunicar na rede e passam a estendê-la para limites imensamente maiores do que a internet que conhecemos atualmente.

Neste livro, vamos contar um pouco dessa história, aprofundar os conhecimentos sobre os conceitos e as definições da Internet das Coisas, ou “Internet of Things – IoT”, como é mais conhecida. Veremos quais normas e padrões estão sendo criados e dão as bases do seu crescimento, impulsionado por um novo protocolo de comunicação da internet, o IPv6.

Organismos internacionais estão criando os padrões para que a IoT tenha interoperabilidade, e, para isso, definiram sua arquitetura geral e as funcionalidades que caracterizam a “coisa” para que seja considerada um componente da rede. Essas características, por sua vez, permitem toda uma gama de desenvolvimento de soluções, que demandam projetos de *design* e atenção específicos, diferentes dos projetos de objetos convencionais.

Essas novas soluções de aplicações para a IoT estão criando mercados novos e de proporções inimagináveis. Fala-se em bilhões de dólares, e cada nova pesquisa de mercado mostra horizontes amplos e algumas vezes inusitados. Soluções de rede “máquina para máquina”, monitoramento remoto de grandezas, objetos de uso pessoal, roupas, esportes, cidades inteligentes, medição inteligente de água e energia, automação predial e residencial, óculos de visão virtual, jogos interativos, são muitas as aplicações que estão nascendo e várias já em operação.

Mas um campo tão vasto como a Internet das Coisas promete surpresas, pois ainda não sabemos os domínios que serão abertos daqui para frente. Neste trabalho, queremos entender e aprofundar um pouco mais tais domínios, e, quem sabe, fazer parte dessa fronteira de descobertas.

Glossário e Acrônimos

0-Touch Network – Rede com funções inteligentes para simplificar o seu gerenciamento em benefício dos usuários e provedores.

Address – “Endereço” de um dispositivo na rede.

API – Application Programming Interface (interface de programação entre aplicações).

Application, App, Aplicação – *software* que implementa lógica de negócios, capaz de prover serviços e processos. Uma aplicação pode estar em um dispositivo, em um sistema empresarial ou na nuvem.

ARP - Address Resolution Protocol.

Atuador – Dispositivo capaz de mover ou controlar um mecanismo ou sistema.

BACNET – Building Automation and Control NETworks (protocolo de comunicação para rede de controle e automação predial).

BICSI - Building Industry Consulting Service International.

CANbus - Controller Area Network, protocolo padrão de comunicação em rede do tipo barramento, originalmente para uso na comunicação de microcontroladores veiculares e dispositivos, sem a necessidade de um computador central, e que ampliou seu uso para diversas outras aplicações industriais.

Cloud – Conceito que define a computação em “nuvem”, ou seja, utilização de memória e processamento compartilhado entre servidores na internet.

CLP - Controladora Lógica Programável.

DCIM – Data Center Infrastructure Management.

Device, dispositivo – Componente físico (*hardware*) com processamento e capacidades de comunicação com sistemas de tecnologia da informação.

DHCP - Dynamic Host Configuration Protocol.

DNS - Domain Name System.

DSL – Digital Subscriber Line, ou linha digital de assinante.

EIA – Electronic Industry Association (Estados Unidos).

EPC – Electronic Product Code, código de produto com mecanismo de endereçamento de identificação universal de produtos físicos, especialmente para tags de RFID.

Gadget – Dispositivos com função específica e prática, útil no cotidiano, tais como: dispositivos eletrônicos portáteis, celulares, MP3, entre outros.

Gateway – Dispositivo capaz de fazer a tradução entre diferentes protocolos, como, por exemplo, para permitir a comunicação entre dispositivos ou subsistemas da IoT e a rede IP da Internet.

HTTP – HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto em sistemas hipermídia), base de comunicação de dados da World Wide Web.

Hz – Hertz (unidade de frequência), e seus múltiplos: kHz – quilohertz (1.000 Hz); MHz – megahertz (1.000.000 Hz) e GHz – gigahertz (1.000.000.000 Hz).

IEEE – Institute of Electrical and Electronic Engineers.

IoT – Internet of Things (Internet das Coisas).

IP - Internet Protocol.

IPsec - Internet Protocol Security, protocolo para garantir segurança em pacotes IP.

IPv4 - Internet Protocol version 4.

IPv6 - Internet Protocol version 6.

ISO – International Organization for Standardization.

ISP - Internet Service Provider (provedor de serviços de internet).

ITU – International Telecommunication Union.

M2M – Machine-to-Machine.

MODBUS – Protocolo de comunicação serial desenvolvido em 1979 pela Modicon, que acabou por se transformar em um protocolo de comunicação padrão. Permite a comunicação entre diversos dispositivos numa mesma rede de automação.

NDP - Neighbor Discovery Protocol, protocolo utilizado com o IPv6.

NFC – Near Field Communication, tecnologia que permite a troca de informações sem fio pela proximidade de diferentes dispositivos/objetos.

OSI - Open Systems Interconnection (modelo aberto de interconexão de sistemas).

PLC – Power Line Communication, protocolo que permite a comunicação de dados pela rede elétrica de baixa tensão de uso doméstico.

PLC – Programmable Logic Controller (Controladora Lógica Programável - CLP).

PROFIBUS – Process Field Bus, protocolo de comunicação em redes de automação industrial.

Proxy – “Procurador”. Consiste de um sistema ou aplicação responsável por intermediar requisições de clientes por recursos de outros servidores, visando a simplificar e controlar tais requisições.

QoS - Quality of Service, sistema de verificação de qualidade de serviços na internet.

RESTful - REpresentational State Transfer, refere-se a web services que fornecem APIs para permitir acesso a serviços na web.

RFID – “Radio Frequency Identification”, ou identificação por radiofrequência, tecnologia sem fio (wireless) para transferir dados com o objetivo de, automaticamente, identificar e rastrear objetos em que estão afixadas tags RFID.

Roaming – Capacidade de obter conectividade em diferentes localidades e redes, mesmo quando visitante.

RS232 – Protocolo de comunicação serial usado em portas de comunicação serial de computadores, como para a ligação de modems, por exemplo.

RS485 – Protocolo de comunicação serial definido pela TIA em sua norma ANSI/TIA/EIA-485, em que “RS” significa “Recommended Standard”, utilizado em redes de comunicação industrial.

RTU – Remote Terminal Unit (Unidade Terminal Remota).

SCADA - Supervisory Control And Data Acquisition system (Sistema supervisório de aquisição e controle de dados).

Sensor – Dispositivo capaz de coletar/gravar informações de uma entidade ou ambiente.

SMTP – Simple Mail Transfer Protocol, protocolo padrão para envio de e-mails na Internet.

SNMP – Simple Network Management Protocol, é o protocolo padrão da Internet para gerenciamento de dispositivos nas redes IP.

Tag – Etiqueta, em sistemas RFID, utilizada para identificar o objeto físico em que está afixada.

TIA – Telecommunication Industry Association (Estados Unidos).

UHF – Ultra High Frequency.

VOIP – Voice Over IP, ou sistema de comunicação de voz sobre protocolo IP.

Capítulo 1

Fundamentos

História

A “internet das coisas” surgiu recentemente como um novo conceito de “rede”, que abrange comunicações e processamento dos mais diversos equipamentos. A palavra “internet”, com o poder simbólico que tem para toda a população mundial, veio para incorporar a nova expressão “internet das coisas”, e, assim, dar a ela abrangência, compreensão imediata de magnitude, tecnologia e perspectivas de futuro.

IoT – *Internet of Things*[1] – como a internet das coisas é mais conhecida -, é uma nova visão para a internet, em que a internet passa a abarcar não só computadores, como, também, objetos do dia a dia. (MATTERN; FLOERKEMEIER, 2010; FACCIONI FILHO, 2016b). Não se trata exatamente de uma nova tecnologia, mas da nova fronteira em que a internet está se aprofundando. Isso é resultado do avanço tecnológico que vem se realizando continuamente, especialmente da miniaturização eletrônica e dos protocolos diversos de comunicação. (HINER, 2013; VERMESAN; FRIESS, 2014).

São inúmeras as aplicações vislumbradas pela IoT. Atualmente, muito se fala em telemetria, aplicações com coleta de dados em ambientes diversos, possibilidade de atuação direta sobre objetos de todos os tipos, relacionamento em rede e interação de objetos entre si[2], interação entre objetos e pessoas, seja de forma provocada ou transparente. (FACCIONI FILHO, 2016b).

A IoT está diretamente associada a outro fenômeno, conhecido por “big data”, nome calcado na expressão da origem do universo, “big bang”, em que uma expansão inimaginável de dados está em processo. Tais dados são gerados e coletados por objetos e computadores, numa relação interativa sem precedentes, indicando um volume para memorizar e processar, com exigências de latência mínima e disponibilidade ininterrupta.

A possibilidade da internet das coisas ocorre com um avanço específico do protocolo da internet, em que cada equipamento pode ter seu “endereço IP”, ou seja, um identificador que permite ser encontrado por qualquer outro equipamento conectado à internet. O protocolo vigente até há pouco, conhecido por IPv4 (*Internet Protocol version 4*), permitia um máximo de 4,3 bilhões de endereços ($4{,}3\times10^{9}$). Esse limite se esgotou, o que quer dizer que novos computadores e equipamentos já não poderiam mais ser conectados à rede simplesmente por não terem um “endereço” na internet. Devido a tal indisponibilidade, a *Internet Engineering Task Force* (IETF) desenvolveu uma nova versão, denominado *Internet Protocol version 6* (IPv6). Essa é a mais recente versão do Protocolo IP, para a identificação e localização de computadores e quaisquer outros objetos ou dispositivos em rede, permitindo o roteamento na internet. Esse protocolo IPv6 utiliza endereço de 128 bits, que permite cerca de $3{,}4\times10^{38}$ endereços IP. (FACCIONI FILHO, 2016b).

1. Dependendo da expressão, usaremos as palavras “coisa” e “objeto” de forma similar ao mencionar a IoT.
2. M2M – Machine-to-Machine.

Dada essa nova característica de endereçamento, praticamente não há limites para quantidades de dispositivos e objetos ligados à internet, o que criou um conjunto de conceitos diferentes (e revolucionários) para suas aplicações, antes relacionadas à imagem de computadores numa rede razoavelmente "restrita".

Mas a história da IoT começa muito antes da Internet. Suas raízes estão na tecnologia RFID – *Radio Frequency Identification*, atualmente utilizada em inúmeras aplicações de etiquetas de identificação de caixas, roupas etc. Os princípios da tecnologia RFID vêm da Segunda Guerra Mundial, como a forma de identificar se o avião captado pelo radar é amigo ou inimigo. O avião, ao captar o sinal do radar, deveria refletir o sinal com as suas características (sistema passivo), ou emitir um novo sinal (sistema ativo), e, assim, permitir ao radar compreender se fazia parte, ou não, de um determinado grupo. (MINERVA; BIRU; ROTONDI, 2015).

Avanços nas tecnologias de radar e de rádio frequência (RF) continuaram após a Segunda Guerra Mundial, e aplicações comerciais foram desenvolvidas para, por exemplo, evitar roubos em lojas com etiquetas de RFID, com resposta simples de 1-bit. A etiqueta responde a um sinal de determinada frequência com resposta "0" ou "1". No caixa, a etiqueta do produto é identificada e o cliente pode passar pelas portas sem acionar o alarme. Caso a etiqueta não tenha sido identificada no caixa, ao passar pelas portas de saída, o alarme será disparado pelo sistema antirroubo. (MINERVA; BIRU; ROTONDI, 2015).

Em 1973, o empreendedor californiano Charles Walton desenvolveu um sistema de controle de acesso sem chaves, baseado em radiofrequência. Basicamente, funcionava com um cartão contendo um *Transponder*[3]. Ao aproximar o cartão da porta que contém o leitor do sinal, é feita a verificação de sua identidade e, então, a porta é desbloqueada.

Também nos anos 1970, no Los Alamos National Laboratory, o governo norte-americano desenvolveu pesquisas para criar identificadores de equipamentos militares e apoiar a logística de transporte e armazenamento, em especial de armas nucleares. Sistemas de RFID foram desenvolvidos para utilização em portões e caminhões de transporte, com *transponders* contendo identificações dos produtos e outras informações. Na mesma época, foram desenvolvidos, nesse laboratório, produtos de identificação em baixa frequência (125 kHz), para rastreamento do gado e sua medicação. Esse sistema de baixa frequência funcionava de forma passiva, ou seja, a resposta do *transponder* se dava com a energia do sinal de rádio recebido. (MINERVA; BIRU; ROTONDI, 2015). Posteriormente, sistemas com frequências mais altas foram desenvolvidos. Há diversos modelos em uso até os dias de hoje, especialmente em soluções de controle de acesso predial.

Frequências mais altas, da ordem de MHz ou mesmo GHz, permitem respostas mais rápidas e maior distância entre o objeto e o leitor.

Em 1999, foi estabelecido, no Massachusetts Institute of Technology (MIT), o centro de estudos Auto-ID Center, que passaria a ser chamado de Auto-ID Labs, após 2003. Esse centro de estudos foi criado com o suporte das seguintes organizações: Uniform Code Council, EAN International, Procter & Gamble e Gillette. Dois professores trabalharam nesse centro, David Brock e Sanjay Sarma, com o intuito de obter etiquetas de RFID com microchips de custo muito baixo e, assim, permitir a expansão rápida desses sistemas. (MINERVA; BIRU; ROTONDI, 2015). O propósito dos seus estudos era de conectar as etiquetas de RFID, chamadas de "tags", com a internet, o que mudou profundamente a ideia

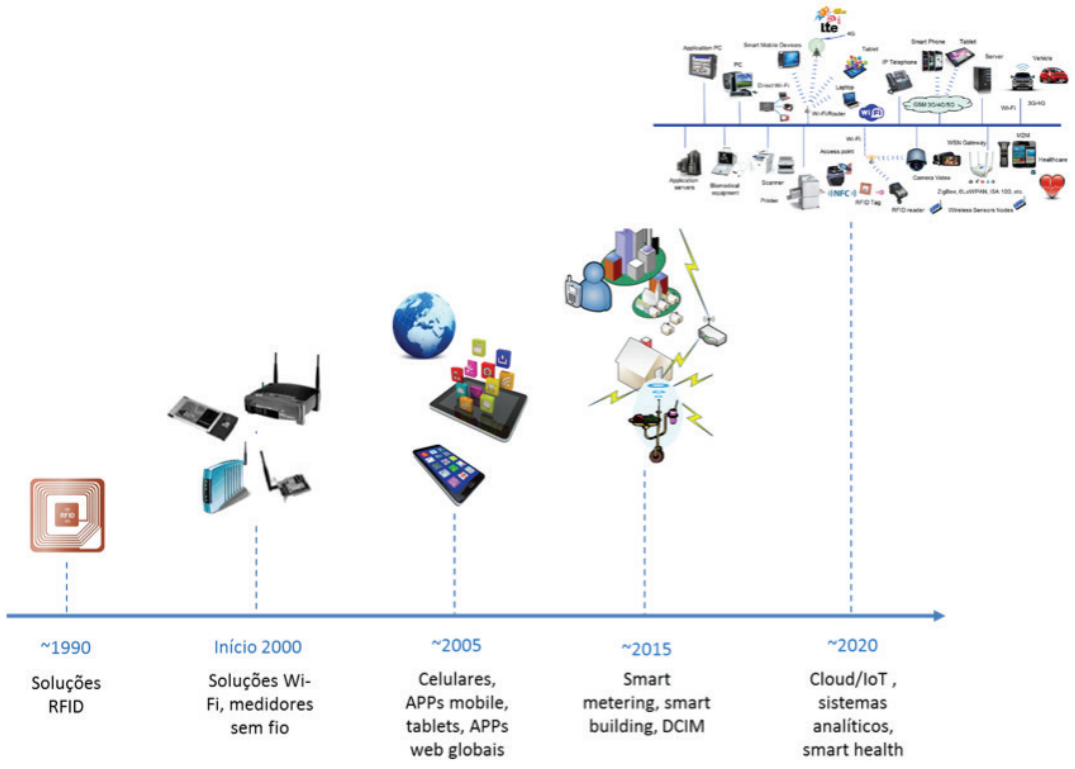
3. Abreviação de Transmitter-responder, dispositivo que recebe um sinal de rádio e, automaticamente, responde com outro sinal de rádio.

das companhias em relação a esse sistema de identificação, pois possibilitaria conhecer, em tempo real, *on-line*, toda a movimentação de cargas e produtos. Essa evolução tecnológica e conceitual motivou mais de 100 grandes empresas e departamentos governamentais americanos a aderirem e suportarem as pesquisas. Essa movimentação, relacionada à utilização do RFID e conexões com a internet, lança as raízes do que seria, logo após, denominado "internet das coisas". (MATTERN; FLOERKEMEIER, 2010; FACCIONI FILHO, 2016b).

Também no MIT, em 1999, no laboratório Media Lab, Neil Gershenfeldt lança o livro "When Things Starts to Think", em que ele escreve: "as coisas começam a usar a Net". Em 2002, na revista Forbes Magazine, o pesquisador do Auto-ID Center, Kevin Ashton, usa a expressão "internet of things" pela primeira vez. (FACCIONI FILHO, 2016b).

E a partir de então, a história da IoT se confirma, sendo que em 2008 acontece a primeira conferência internacional sobre o tema da internet das coisas em Zurich, Suiça: First International Conference, IOT 2008[4]. Nessa conferência, são discutidos, em sessões científicas, temas como RFID, sensoriamento, aspectos de negócios e tecnologias de conexão e conversão de protocolos, dando origem a um enorme campo de debates e evoluções técnicas, consolidando o cenário da "internet das coisas", cuja história está resumida na ilustração da Figura 1.1.

Figura 1.1 – Evolução histórica da IoT



Fonte: Adaptação de Barnaghi e Sheth, 2014.

4. O site do evento está ativo em: <http://www.iot-conference.org/iot2008/>. Acesso em: 22 ago. 2016.

Conceitos e definições

A Internet das Coisas é um conceito que está fora do âmbito das tecnologias, pois não deriva delas, e sim as utiliza para cumprir uma série de funcionalidades. As tecnologias associadas ao "conceito" são muitas, e apenas para citar algumas, temos as que se referem à conexão física dos objetos, ou de infraestrutura básica, como as conexões cabeadas e as conexões sem fio[5]. (FACCIONI FILHO, 2016b).

Em termos de protocolos diversos e capazes de expandir a nova "rede de objetos", há ainda protocolos tradicionais do ambiente industrial e predial[6], pois os objetos existentes e já operando em tais sistemas não só podem como serão envolvidos na grande rede de interligação de objetos.

As funcionalidades do objeto na IoT já estão postas pelo mercado e pelas organizações normativas, e as tecnologias associadas continuam em desenvolvimento. Diversos fabricantes da área de equipamentos eletrônicos e computacionais estão num esforço para criar sua linha de produtos e dispositivos para IoT, tais como Cisco, Intel e muitos outros. A **Intel**, que fabrica os componentes para a funcionalidade de "processamento" dos objetos, definindo assim suas características, acredita em "intelligent devices to deliver intelligence where needed and to acquire and filter data from the field"[7]. (FACCIONI FILHO, 2016b). Esses equipamentos irão compor sistemas inteligentes, integrando bilhões de dispositivos e provendo soluções e análises para valorizar soluções fim a fim dos clientes. (SKARPNESS, 2014).

Pelo lado dos desenvolvedores de aplicações, há uma multiplicação de novas soluções, e novas expressões podem ser citadas: smart buildings, smart cities, smart transport, smart grid, smart energy, smart health, entre outras (FACCIONI FILHO, 2015). Essas soluções são apenas a superfície do que está sendo preparado para o futuro próximo, e o design de produtos digitais e de plataformas IoT deverá se ajustar a esses novos paradigmas.

De acordo com Minerva, Biru e Rotondi (2015), a IoT é um domínio que integra diferentes tecnologias e campos sociais e de negócios, como ilustrado na Figura 1.2.

5. Wi-Fi e WLAN, Bluetooth, RFID, NFC, ZigBee, entre outras.

6. Como: CanBus, ModBus, ProfiBus, BacNet e muitos outros.

7. "Equipamentos inteligentes para entregar inteligência onde necessário, e para coletar e filtrar dados de campo".

Figura 1.2 – Domínios tecnológicos e de negócios da IoT

Fonte: Adaptação de Minerva, Biru e Rotondi, 2015.

Ainda não há uma definição estabelecida da Internet das Coisas, tal a diversidade de elementos que a compõe. Na figura 1.2, pode-se verificar um grande conjunto de áreas que são cobertas pela IoT. Componentes de "baixo nível"[8] fazem parte de uma camada de base que se espalha pelos mais diversos ambientes. Há um conjunto de *softwares* que integra tais componentes, passando por sistemas operacionais, protocolos de comunicação, aplicações, interfaces, bancos de dados e sistemas em nuvem. Essa camada de *software* é essencial para o sucesso da IoT, inclusive, ao tratar de agentes autônomos capazes de autogestão e autoidentificação ao integrarem aplicações, pois o número de componentes em uma determinada plataforma pode facilmente chegar aos milhões. Deriva disso a questão crítica da privacidade e da segurança na IoT, que são fundamentais ao envolver negócios e relações comerciais.

» O impacto da IoT chega justamente nisso, aos negócios, pois uma série de novas oportunidades e modelos de negócios precisam ser criados e estabelecidos, que também se darão no campo social e individual.

Para chegar, se chegar, a uma definição da Internet das Coisas, e diferenciá-la de outras redes de sistemas interconectados, podemos partir do conjunto de funcionalidades e características do objeto (ou "coisa"), que tanto pode ser físico quanto virtual. Isso define a IoT como um sistema complexo e também suporta a criação e o design dos objetos, dos subsistemas e dos processos internos da IoT. (FACCIONI FILHO, 2016a).

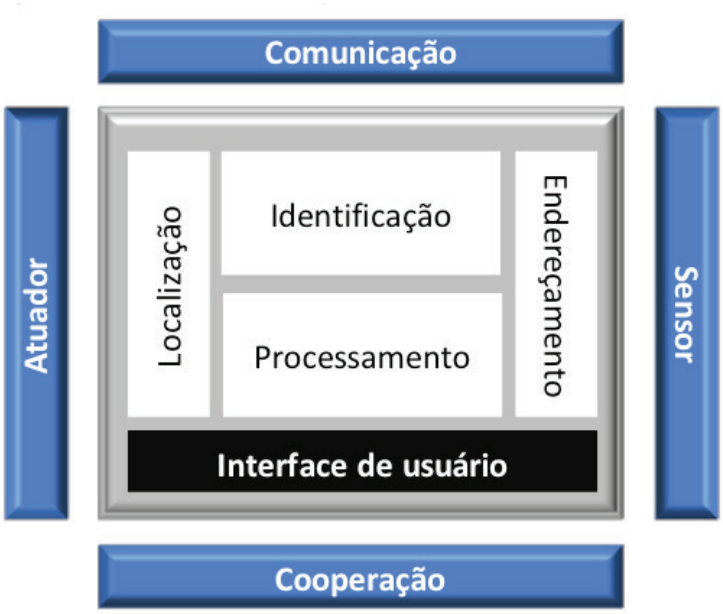
8. Como: sensores, coletores de dados, medidores de energia etc.

As funcionalidades de um objeto pertencente à internet das coisas são nove, distribuídas em três conjuntos, conforme topologia na Figura 1.3. (FACCIONI FILHO, 2016b):

- Características
- Relações
- Interface

Nem todas essas funcionalidades precisam estar presentes no objeto simultaneamente, pois dependem do uso de cada objeto e das aplicações em que estão inseridos. Apresentaremos, aqui, uma visão geral dessas funcionalidades, que detalharemos depois no capítulo das Tecnologias da IoT.

Figura 1.3 – Funcionalidades do Objeto na Internet das Coisas



Fonte: Elaboração do autor, 2016.

O conjunto das características é composto das atribuições do próprio objeto, o conjunto das relações refere-se a como o objeto interage com outros objetos em rede e o conjunto da interface refere-se às relações entre o objeto e o usuário.

No **conjunto das características** do objeto na IoT, existem as seguintes atribuições (FACCIONI FILHO, 2016b):

- **Processamento**, que se refere à capacidade de processamento computacional inserida no objeto, ou "inteligência", capaz de fazê-lo agir e responder às requisições da IoT e às suas aplicações;
- **Endereçamento**, que se refere à capacidade do objeto de ser encontrado na IoT, ou seja, de ser localizado na rede por meio do roteamento;
- **Identificação**, que se refere à identidade de cada objeto, fazendo-o único em toda a rede IoT;
- **Localização**, atributo relacionado ao local físico em que o objeto se encontra, à sua posição no mapa geográfico.

No **conjunto das relações** com outros objetos na IoT, existem as seguintes funcionalidades:

- **Comunicação**, que é a capacidade do objeto de receber e/ou enviar mensagens para outros objetos na IoT;
- **Cooperação**, que se refere à capacidade do objeto de agir em comum com outros objetos da IoT, visando a atividades e aplicações cooperadas, ou seja, ações conjuntas e de colaboração;
- **Sensoriamento**, que é a capacidade do objeto de captar dados do ambiente ou de outros objetos, dados esses obtidos por meio de sensores presentes no próprio objeto e que permitem monitorar determinadas grandezas do ambiente;
- **Atuação**, que é a capacidade do objeto de agir sobre o ambiente, operando e modificando a condição de um determinado meio.

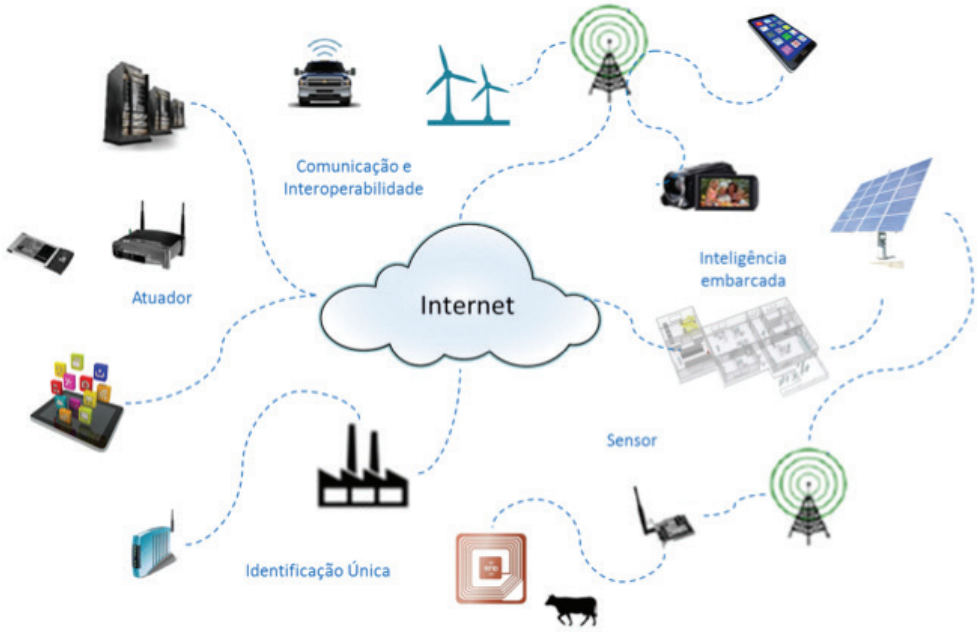
O **conjunto da interface** refere-se à interação do objeto com o usuário, permitindo-lhe visualizar informações do objeto, realizar configurações e modificar sua condição.

Partindo dessas características e funcionalidades, considerando que a Internet das Coisas pode compreender sistemas complexos e com milhões de objetos e interconexões, executando inúmeros processos em diversos níveis e subníveis, a seguinte definição de IoT é proposta em Minerva, Biru e Rotondi (2015, p. 74):

> A IoT – Internet of Things – compreende uma rede complexa, adaptativa e autoconfigurável, que interconecta “coisas” à Internet por meio de protocolos de comunicação normatizados. As “coisas” interconectadas têm representação física ou virtual no mundo digital, capacidade de atuação/sensoriamento, funcionalidade de programação e identificação única. Tal representação contém informações da identidade, status, localização e informações privadas ou sociais relevantes da “coisa”. A “coisa” oferece serviços, com ou sem intervenção humana, por meio de identificação única, coleta de dados, comunicação e capacidade de atuação. A exploração dos seus serviços se dá pelo uso de interfaces inteligentes e pode ser feita de qualquer lugar, a qualquer tempo e com segurança.

De acordo com esta definição, a Figura 1.4 apresenta uma visão geral do escopo da IoT.

Figura 1.4 – Escopo da IoT



Fonte: Elaboração do autor, 2016.

Protocolo IPv6

Um dos grandes problemas da Internet é fruto justamente do seu sucesso. A sua enorme expansão, e que aparentemente ainda está no início, deu origem a problemas de identificação dos equipamentos conectados à rede, considerando a quantidade crescente de dispositivos. O advento da Internet da Coisas traz um ingrediente novo a esse ambiente, com uma imensa carga de novos dispositivos buscando entrar na “rede” e atuar nela, e, para isso, esses dispositivos precisam ter identificação, ou seja, um endereço para que sejam “encontrados” na rede.

Na internet, essa identificação, ou “endereço IP”, foi definida pelo protocolo de identificação chamado IPv4 (*Internet Protocol version 4*), que permite um máximo de aproximadamente 4,3 bilhões de endereços ($4{,}3\times10^9$). Essa quantidade de endereços foi totalmente utilizada até o ano de 2015, por esse motivo, a expansão da internet estaria comprometida a partir de então. Dessa forma, a *Internet Engineering Task Force* (IETF) partiu para o desenvolvimento de uma nova versão de protocolo de identificação, que foi denominado *Internet Protocol version 6* (IPv6).

No Brasil, a responsabilidade do endereçamento é do Comitê Gestor da Internet - CGI.br, que coordena a Internet no país. O CGI criou, para implementar suas decisões e projetos, o Núcleo de Informação e Coordenação do Ponto BR, conhecido por NIC.br, o qual englobou as iniciativas para essa mais recente versão do Protocolo IP, que chamou de IPv6.br, e, assim, a identificação e localização de computadores e quaisquer outros objetos ou dispositivos em rede, permitindo o roteamento na Internet com o *Internet Protocol version 6* (IPv6).

De acordo com Moreiras et al (2015), a Internet desenvolveu-se com dois protocolos:

1. o TCP - *Transmission Control Protocol*
2. o IPv4

As funções do IPv4 eram de endereçamento lógico, segmentação, priorização de pacotes e descarte dos pacotes com problemas. Os endereços IPv4 são de 32 bits, os quais são divididos em quatro grupos, cada grupo com 8 bits, escritos com dígitos decimais[9], atingindo o máximo de 4,3 bilhões de endereços. O novo IPv6 divide o endereço em oito grupos de 16 bits cada (total de 128 bits), escritos com dígitos hexadecimais (0-F)[10]. Isso permite cerca de $3{,}4 \times 10^{38}$ endereços IP (FACCIONI FILHO, 2016). Dada essa nova característica de endereçamento, praticamente não há limites para quantidades de dispositivos e objetos ligados à internet, o que criou um conjunto de conceitos diferentes (e revolucionários) para suas aplicações, antes restrita à concepção de que haveria apenas computadores numa rede razoavelmente "restrita". A IoT tira proveito disso para possibilitar a expansão da Internet.

No protocolo IPv6, há alguns endereços descritos como:

- Unicast – para identificar uma única interface na internet, ou seja, o pacote enviado para esse endereço será entregue para uma única interface, ou seja, comunicação "um-para-um";
- Anycast – para identificar um conjunto de interfaces, sendo que o pacote enviado para esse endereço será entregue para a interface pertencente a esse conjunto e que se encontra mais próxima da origem (proximidade que se mede pelos protocolos de roteamento), definindo uma comunicação de "um-para-um-de-muitos";
- Multicast – para identificar um conjunto de interfaces, sendo que o pacote enviado para esse endereço será entregue para todas as interfaces desse conjunto, ou seja, uma comunicação "um-para-muitos".

9. Como, por exemplo, 192.168.0.10.

10. Como, por exemplo, 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1.

As principais diferenças entre IPv4 e IPv6 estão resumidas no seguinte Quadro 1.1, em que se evidenciam as aplicações para a Internet das Coisas:

Quadro 1.1 – Comparações entre protocolos IPv6 e IPv4

	IPv4	IPv6
Número de endereços IP	$4{,}3\times10^{9}$	$3{,}4\times10^{38}$
Dimensão do endereço	32 bits	128 bits
Suporte Ipsec	Opcional	Obrigatório
Capacidade de QoS	Não	Sim, no campo Flow Label
Fragmentação da informação	Realizada nos roteadores	Processada no host
Resolução de endereçamento	Protocolo ARP utiliza broadcast	Não tem ARP, usa protocolo "Neighbor Discovery"
Enderaçamento Broadcast	Broadcast para todos os host da rede	Não usa Broadcast, usa Multicast
Configuração	Endereço configurado manualmente	Funcionalidades de autoconfiguração
Pacotes	Suporta pacotes de 576 Bytes, que podem ser fragmentados	Suporta pacotes de 1280 Bytes, sem fragmentação
Internet das Coisas	É usado, mas não é apropriado	É apropriado e permite a expansão da IoT

Fonte: Adaptação de Holanda, 2016.

Normas da IoT

Apesar de a IoT não ser especificamente uma nova tecnologia, e sim um conceito que integra diversas tecnologias e plataformas, a sua existência e expansão dependem de um conjunto de normas e padrões que inter-relacionam tais tecnologias. Esses padrões acabam por gerar parâmetros que permitem a melhoria técnica dos sistemas, e, a partir disso, a criação de novos produtos, aplicações e plataformas. As normas internacionais são a base sobre a qual a IoT se fundamenta e poderá se expandir.

De acordo com Minerva, Biru e Rotondi (2015), as mais diversas organizações estão empenhadas em criar normas para a IoT (standards), porém, algumas delas podem ser destacadas. As definições de IoT mais importantes estão sendo propostas pelas organizações:

- **IEEE** – Institute of Electrical and Electronic Engineers;
- **ETSI** - European Telecommunications Standards Institute;
- **ITU** – International Telecommunications Union;
- **IETF** - Internet Engineering Task Force;
- **NIST** - National Institute of Standards and Technology;
- **W3C** - World Wide Web Consortium.

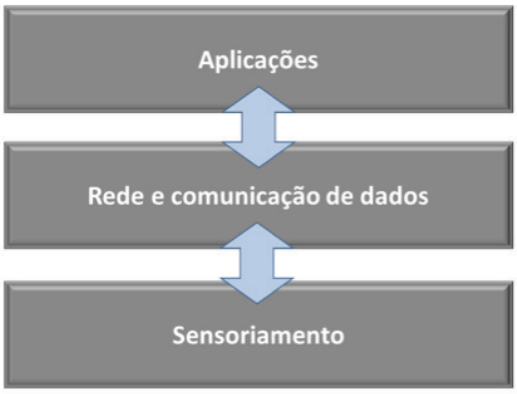
Vamos a seguir apresentar algumas dessas propostas de normas que deverão guiar os caminhos da IoT no futuro próximo.

IEEE – Institute of Electrical and Electronic Engineers

O Instituto IEEE é uma associação global que atua há décadas no fomento da tecnologia e na definição de normas[11]. De acordo com o IEEE, um conceito não oficial de Internet das Coisas seria: "Uma rede de dispositivos – cada um com sensores embutidos – que são conectados à Internet." (MINERVA; BIRU; ROTONDI, 2015, p. 10).

Entre vários grupos de trabalho do IEEE relacionados à IoT, o que está diretamente focado na Internet das Coisas é o de número IEEE P2413[12], cujo escopo é definir uma arquitetura estrutural da IoT, com seus domínios, abstrações e pontos comuns. Atualmente, essa arquitetura é constituída de três níveis, Aplicações, Rede/Comunicação de Dados, e Sensoriamento, conforme ilustrado na Figura 1.5.

Figura 1.5 – Arquitetura da IoT conforme a IEEE P2413



Fonte: Elaboração do autor, 2016.

Os objetivos do grupo de trabalho IEEE P2413 são os seguintes:

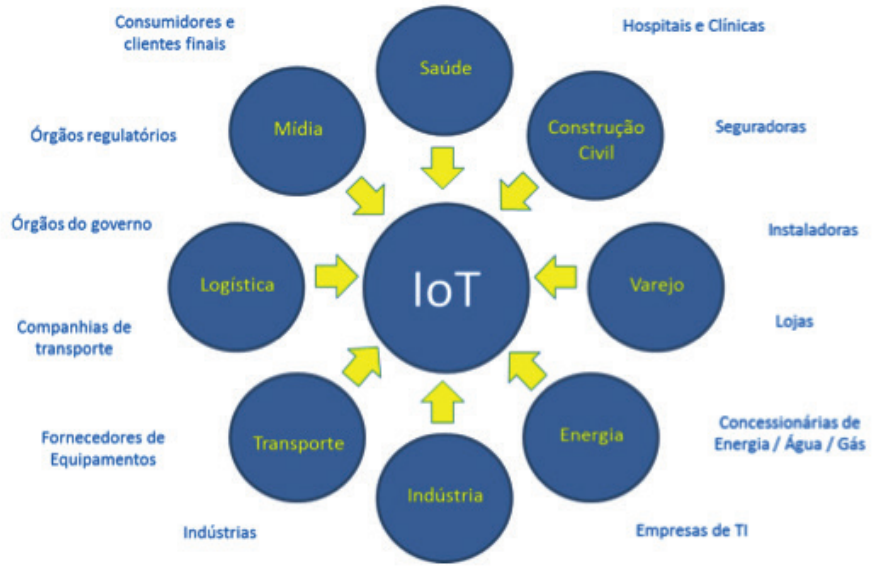
- definir uma arquitetura estrutural capaz de cobrir diferentes necessidades das diversas aplicações da Internet das Coisas;
- acelerar o crescimento do mercado de IoT permitindo interações entre diferentes domínios e tecnologias, bem como a unificação de plataformas por meio da compatibilidade entre sistemas, interoperabilidade e intercâmbio de funcionalidades;
- ampliar a transparência entre estruturas dos sistemas IoT, de modo a suportar avaliações comparativas e de segurança;
- reduzir a fragmentação do mercado e criar uma massa crítica de atividades colaborativas por todo o mundo;
- intensificar o atual conjunto de trabalhos em IoT.

11. Tais como os Standards para a Ethernet, Wi-Fi e muitas outras tecnologias que fazem parte do nosso dia a dia.

12. P2413 - Standard for an Architectural Framework for the Internet of Things – IoT.

De acordo com a visão do IEEE P2413, a Figura 1.6 ilustra o conjunto de participantes e interessados no mercado da IoT:

Figura 1.6 – Mercado e participantes do ecossistema da IoT



Fonte: Elaboração do autor, 2016.

ETSI - European Telecommunications Standards Institute

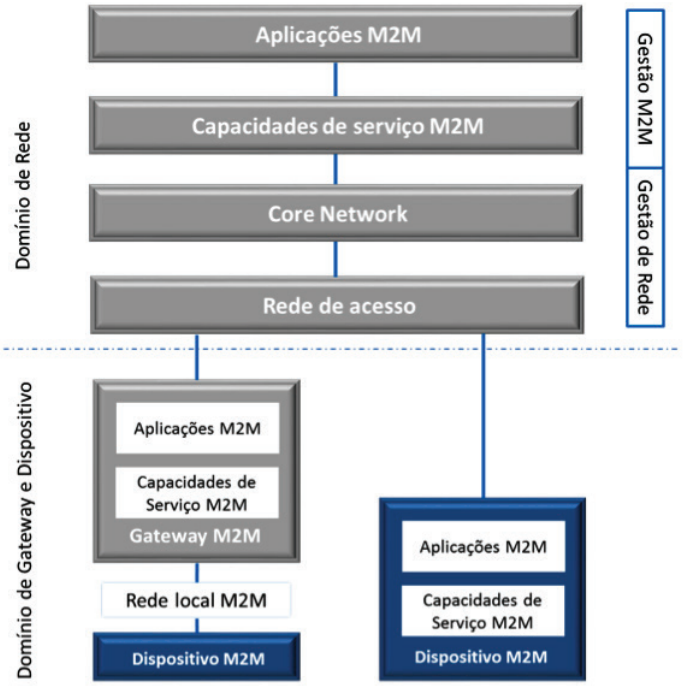
O Instituto ETSI é reconhecido pela União Europeia (RU) como uma organização de especificação de normas da Europa, ele produz standards em tecnologias de comunicação e informação, incluindo as diversas tecnologias associadas à internet e sua infraestrutura. Apesar de a ETSI não citar a expressão “Internet das Coisas” em seus documentos, ela utiliza um conceito similar descrito como “M2M – Machine to Machine”, que tem sido muitas vezes confundido com a IoT, pois é comum nos referirmos a dispositivos M2M como “coisas” da IoT.

Para a ETSI (MINERVA; BIRU; ROTONDI, 2015, p. 12), a:

> Comunicação Machine-to-Machine (M2M) é a comunicação entre duas ou mais entidades que não necessariamente precisam da intervenção humana para ocorrer; serviços M2M devem automatizar processos de decisão e comunicação.

O ETSI criou uma arquitetura da comunicação M2M, que é ilustrada na Figura 1.7:

Figura 1.7 – Modelo da arquitetura M2M de acordo com a ETSI



Fonte: Adaptação de Minerva, Biru e Rotondi, 2015.

Nela, são apresentadas as suas **entidades lógicas**, descritas a seguir (MINERVA; BIRU; ROTONDI, 2015):

- **M2M Device**: dispositivo/objeto que roda aplicações M2M utilizando funcionalidades M2M, e conecta ao domínio da rede de duas maneiras:
  - **Conectividade direta**: dispositivos/objetos M2M conectam ao domínio da rede pela rede de acesso, executando procedimentos como registro, autenticação, gestão e provisionamento.
  - **Gateway**: dispositivos/objetos M2M conectam ao domínio da rede por meio de gateways M2M, em que os gateways atuam como "proxy", executando serviços de autenticação, autorização, gestão em provisionamento.
- **M2M Area Network**: provê conectividade entre dispositivos/objetos M2M e gateways M2M.
- **M2M Gateway**: gateway que roda aplicações M2M utilizando funcionalidades M2M. Atua como um proxy entre os dispositivos M2M e o domínio de rede, e pode prover serviços para outros dispositivos conectados nele e que não são visíveis para a rede.
- **Access Network**: a rede de acesso permite que dispositivos M2M e gateways M2M comuniquem com o núcleo da rede.
- **Core Network**: núcleo da rede, a qual provê no mínimo a conectividade IP com a internet, além de outras possibilidades de conexão, serviços, funcionalidades, interconexões e roaming.

- **M2M Service Capabilities**: aplicações que rodam serviços lógicos e usam capacidades de serviço acessíveis por interfaces abertas.
- **Network Management Functions**: todas as funcionalidades necessárias para gerir as redes de acesso e o núcleo da rede, o que inclui supervisionamento, detecção de falhas, provisionamento e outros.
- **M2M Management Functions**: todas as funcionalidades necessárias para gerir os serviços M2M no domínio da rede.

O ETSI contribui ainda para outra iniciativa, denominada **OneM2M Global Initiative**, que se constitui como uma parceria global entre empresas e organizações para a criação de normas voltadas à M2M, visando a implementações em larga escala na IoT.

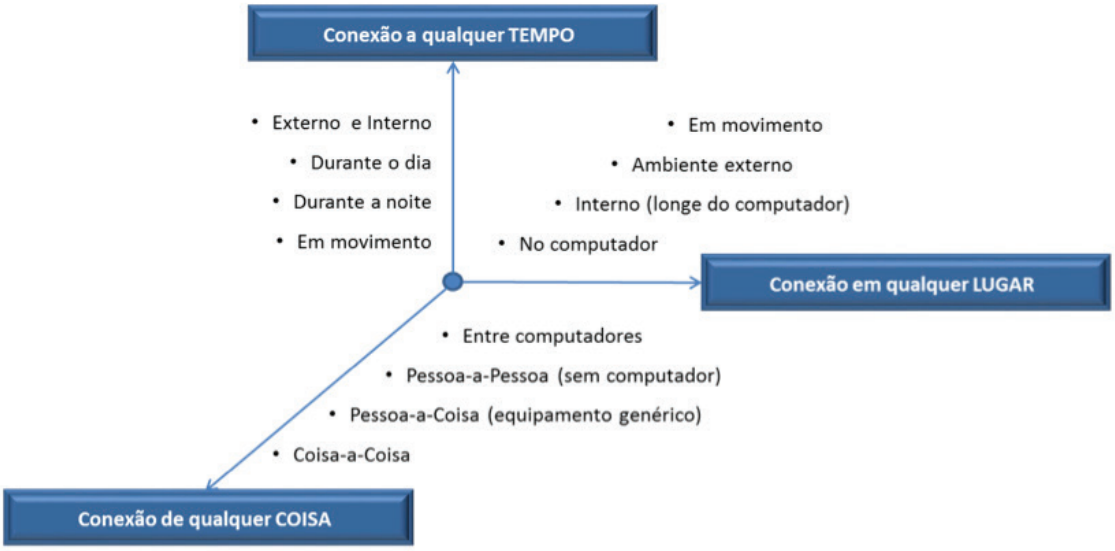
ITU - The International Telecommunication Union

A ITU é a agência especial das Nações Unidas para questões relacionadas a tecnologias da informação e comunicação (TIC). É a ITU que faz a alocação global dos espectros de rádio e órbitas de satélites, desenvolve normas e busca prover acesso para as tecnologias da informação e comunicação para comunidades de todo o mundo, em especial as menos favorecidas.

Em 2005, a ITU descreveu a IoT como uma "rede ubíqua", ou seja, rede onipresente, em que a rede e a conectividade são disponíveis em todos os lugares e a qualquer tempo. Assim, conforme Minerva, Biru e Rotondi (2015, p. 17), a ITU criou sua definição de Internet das Coisas como a rede "disponível em qualquer lugar, a qualquer momento, por qualquer coisa e por qualquer pessoa."

A Figura 1.8 ilustra essa definição da ITU:

Figura 1.8 – Definição de IoT



Fonte: Adaptação de Minerva, Biru e Rotondi, 2015.

O Grupo de Estudos 13 da ITU, posteriormente, criou uma definição mais detalhada da IoT, como segue:

> A internet das coisas é uma infraestrutura global para a sociedade da informação, permitindo serviços avançados para interconectar coisas (físicas e virtuais), baseados em tecnologias de comunicação e informação existentes e em desenvolvimento.

Complementa a definição com as seguintes notas:

> Por meio de sistemas de identificação, coleta de dados, processamento e comunicação, a IoT faz uso de coisas para oferecer serviços para todos os tipos de aplicações, assegurando procedimentos de privacidade e segurança. [...]. Numa perspectiva ampla, a IoT pode ser compreendida como uma **visão de sistema** com implicações tecnológicas e sociais. (MINERVA; BIRU; ROTONDI, 2015, p. 19, grifo nosso).

Para possibilitar a existência da IoT, a ITU descreveu as seguintes tecnologias como necessárias:

- **RFID** (para etiquetar as coisas);
- **sensores** (para perceber e coletar informações);
- **inteligência** (para as coisas "pensarem");
- **nanotecnologia** (para miniaturizar as coisas).

Como esses conceitos estão se tornando as bases da IoT, vamos detalhar um pouco mais as definições da ITU.

RFID (as coisas com "tags")

Com o objetivo de conectar objetos comuns e dispositivos diversos às redes, em especial, à Internet, o uso do sistema de identificação simples e barato conhecido como RFID é indispensável. Utiliza-se a palavra "tag" para se referir às etiquetas RFID que estão em embalagens, equipamentos, roupas, aparelhos e muitas outras "coisas". Com uma tag RFID é possível identificar, de maneira única, cada objeto, pois cada tag pode conter, de certa maneira, uma mini base de dados. Não é necessária visada entre o sensor e a tag para que a comunicação se estabeleça, e uma distância de um metro é comum para muitas aplicações, sendo que tags em UHF podem chegar a uma distância muito maior. Essas capacidades da tag RFID possibilitam que qualquer "coisa", objeto, animal ou planta, seja identificado e rastreado, tornando essa "coisa" um nó da Internet.

Sensores (as coisas "sentem")

Um dos pontos fundamentais da IoT é a parte de sensoriamento. Os sensores estão nas raízes do conceito de Internet das Coisas. São dispositivos importantes para coletar informações em campo, em ambientes inacessíveis, em sistemas produtivos, na área médica, na análise de distúrbios, na criação animal e outros inimagináveis processos. Aos sensores muitas vezes se acoplam atuadores, de tal forma que em processos especiais pode-se não só coletar dados

como também atuar sobre o ambiente, como, por exemplo, um sensor de luminosidade que também é capaz de acionar uma lâmpada.

Inteligência (as coisas "pensam")

Com isso, se quer dizer que há capacidade de processamento embutido nas "coisas", tecnologias que atribuem inteligência às extremidades da IoT. Processamento diretamente nas coisas faz com que a inteligência seja distribuída, diminuindo tanto o tráfego na rede como em servidores centrais. Nesses sistemas, há três tipos de inteligência nas coisas:

1. *passiva*: em que o objeto responde a estímulos de maneira direta e sem processar a informação coletada;
2. *ativa*: em que o objeto, a partir de um controlador remoto, pode decidir o tipo de resposta a partir de um estímulo;
3. *autônoma*: em que o objeto carrega em si mesmo a capacidade do controlador, bem como sensor e atuador, decidindo, de forma autônoma, suas ações a partir de estímulos vindos da rede ou do ambiente.

Nanotecnologia (as coisas são "pequenas")

Essa definição parte do princípio de que as coisas na IoT devem ser cada vez menores, com menor consumo de energia, maior velocidade de processamento e maior capacidade de memória, e, por isso, influenciam de maneira radical no design de produtos.

IETF - Internet Engineering Task Force

A IETF é uma comunidade internacional aberta[13] interessada na evolução, operação e independência da Internet. Devido à sua importância para a comunidade relacionada à Internet, sua definição de IoT é fundamental como guia da evolução tecnológica. A IETF apresenta definições da IoT em conjunto com sua visão complementar de Internet e de "coisa":

> A **internet das coisas** irá conectar objetos do nosso entorno (eletrônicos, elétricos e não elétricos) para prover comunicação transparente e serviços contextuais. O desenvolvimento de tags RFID, sensores, atuadores e telefones celulares possibilita a materialização da IoT por interagirem e cooperarem entre si, criando melhores serviços, acessíveis em qualquer lugar e a qualquer momento. [...]. A '**internet'** original é baseada no protocolo TCP/IP, mas nem toda rede que usa a TCP/IP faz parte da internet, pois podem ser redes privadas ou redes de telecomunicações. Do ponto de vista da IoT o termo 'internet' considera redes TCP/IP e redes não TCP/IP ao mesmo tempo. [...]. Considerando a IoT, **coisas** são itens variados como computadores, sensores, pessoas, atuadores, refrigeradores, TVs, veículos, fones celulares, roupas, comidas, remédios, livros, etc. Essas coisas são classificadas em três grupos: pessoas, máquinas (por exemplo sensores, atuadores, etc.) e informação (por exemplo roupas, comida, remédios, livros, etc.) Essas coisas devem ser identificadas pelo menos por um meio único de identificação para possibilitar

13. Da qual participam institutos, projetistas, fabricantes, pesquisadores, designers e organismos diversos.

> endereçamento e comunicação entre elas, com certificação de identidade. Nesse caso, se a 'coisa' for identificável, chamamos de 'objeto'. (MINERVA; BIRU; ROTONDI, 2015, p. 19, grifos nossos).

NIST - National Institute of Standards and Technology

A importância do instituto NIST se dá por sua participação no Departamento de Comércio dos EUA e por ser um dos mais antigos laboratórios de ciências exatas, voltado tanto para as nanotecnologias, como para os sistemas de grandes dimensões, tais como edifícios, ecossistemas e redes globais de comunicação.

Para o NIST, a IoT está inserida no conjunto maior da cibernética, porém, usa os dois termos de forma indistinta. O NIST tem uma definição geral da IoT, desenvolvida, de forma geral, por um grupo de estudiosos denominado "Smart America/Global Cities Challenge", e outra, criada por um dos seus executivos, Chris Greer. A definição da IoT pelo grupo "Smart America/Global Cities Challenge" (MINERVA; BIRU; ROTONDI, 2015, p. 20) é a seguinte:

> Sistemas 'cibernéticos', muitas vezes referindo-se a 'Internet of Things – IoT' – envolve a conexão, de uma nova maneira, de dispositivos e sistemas inteligentes em diversos setores, tais como transportes, energia, manufatura e saúde. Cidades e Comunidades Inteligentes (Smart Cities/Communities) estão progressivamente adotando tecnologias de IoT para aumentar a eficiência e a sustentabilidade de suas operações visando a melhoria da qualidade de vida.

W3C - World Wide Web Consortium

O W3C é um consórcio internacional que reúne membros corporativos e instituições em geral, visando a desenvolver normas relacionadas à Web. O W3C considera a IoT como parte do que chama de WoT, ou Web of Things, outro acrônimo da área das tecnologias. Para o W3C (MINERVA; BIRU; ROTONDI, 2015, p. 21), a definição de WoT é a seguinte:

> A Web of Things – WoT – refere-se essencialmente ao papel que as tecnologias da web desempenham para facilitar o desenvolvimento de aplicações e serviços para a Internet of Things, ou seja, objetos físicos e sua representação virtual. Isso inclui sensores e atuadores, bem como objetos físicos identificados por códigos de barras ou NFC (Near Field Communication). Algumas tecnologias Web relevantes incluem HTTP para acessar serviços RESTful, para nominar objetos como uma base de conexão de dados e descrições enriquecidas, e para APIs JavaScript para atuar em objetos virtuais como proxies de objetos do mundo real.

Certamente, os acrônimos[14] estão se debatendo na tentativa de sobreviver nesse ambiente mutável das tecnologias. Mas a que se firmou é a IoT, especialmente pela preponderância que o instituto IEEE (e seu projeto de norma IEEE P2413) mantém há décadas nas áreas de engenharia, computação e tecnologias de informação e comunicação. As normas da IoT são fundamentais para permitir a pesquisa e o desenvolvimento de produtos e sistemas, e especialmente sua expansão no ambiente da produção industrial e do consumo.

14. Como, por exemplo, o WoT, a Cibernética, a Internet of Everything (IoE, adotada pela Cisco), entre outras.

Nos próximos capítulos, vamos investigar as questões técnicas relacionadas a IoT e como novos produtos e casos práticos estão criando essa nova realidade.

Referências

BARNAGHI, Payam; SHETH, Amit. The Internet of Things: The Story So Far. **IEEE** - Internet of Things. 09 set. 2014. Disponível em: <http://iot.ieee.org/newsletter/september-2014/the-internet-of-things-the-story-so-far.html>. Acesso em: 23 ago. 2016.

FACCIONI FILHO, Mauro. BMS 2.0 - Nova geração de sistemas de automação e gestão predial. **Congresso Netcom,** São Paulo, Aranda Eventos, 2015.

_____. Complex Systems: Risk Model Based on Social Network Analysis. In: **INTERNATIONAL SYMPOSIUM ON INDUSTRIAL ELECTRONICS** (ISIE), 25th, 2016, Santa Clara, CA, USA. 2016a. p. 22-27.

_____. Designing "things" for the Internet of Things. In: **I CONGRESSO INTERNACIONAL, I; WORKSHOP DESIGN & MATERIAIS**, VII, 2016, São Paulo: Universidade Anhembi Morumbi, 2016b.

HINER, Jason. **The Executive´s Guide to the Internet of Things**. ZDNet e TechRepublic, 2013.

HOLANDA, Emanuel. IPv6 x IPv4. **IPv6**. Disponível em: <https://reaipv6.wordpress.com/ipv6xipv4/>. Acesso em: 23 ago. 2016.

MATTERN, Friedemann; FLOERKEMEIER, Christian. From de Internet of Computers to the Internet of Things. In: SACHS, Kai; PETROV, Ilia; GUERRERO, Pablo (Eds.). **From active data management to event-based systems and more**: papers in honor of Alejandro Buchmann on the occasion of his 60th birthday. pp. 242-259, Berlin: Springer, 2010.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. **Towards a Definition of the Internet of Things (IoT)**. IEEE Internet Initiative - Telecom Italia. 27 maio 2015. Disponível em: <https://pt.scribd.com/doc/306069323/IEEE-IoT-Towards-Definition-Internet-of-Things-Revision1-27MAY15>. Acesso em: 23 ago. 2016.

MOREIRAS, Antonio Marcos; SANTOS, Rodrigo Reis dos; HARANO, Alexandre Yukio; CORDEIRO, Edwin Santos; NAKAMURA, Tiago Jun; MORALES, Eduardo Barasal; GANZELI, Heitor de Souza; CARNIER, Rodrigo Matos; LUGOBONI, Gustavo Borges. **Laboratório de IPv6**: aprenda na prática usando um emulador de redes. São Paulo: Novatec, 2015. Disponível em: <http://ipv6.br/pagina/livro-ipv6/>. Acesso em: 23 ago. 2016.

SKARPNESS, Mark. **Preparing the Data Center for the Internet of Things**. Intel Software and Services Group. 13 nov. 2014. Disponível em: <http://pt.slideshare.net/Inteliot/slideshelf>. Acesso em: 23 ago. 2016.

VERMESAN, Ovidiu; FRIESS. Peter (Eds.). **Internet of Things - From Research and Innovation to Market Deployment.** Aalborg: River Publishers, 2014. Disponível em: <http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf>. Acesso em: 23 ago. 2016.

Capítulo 2

Tecnologia

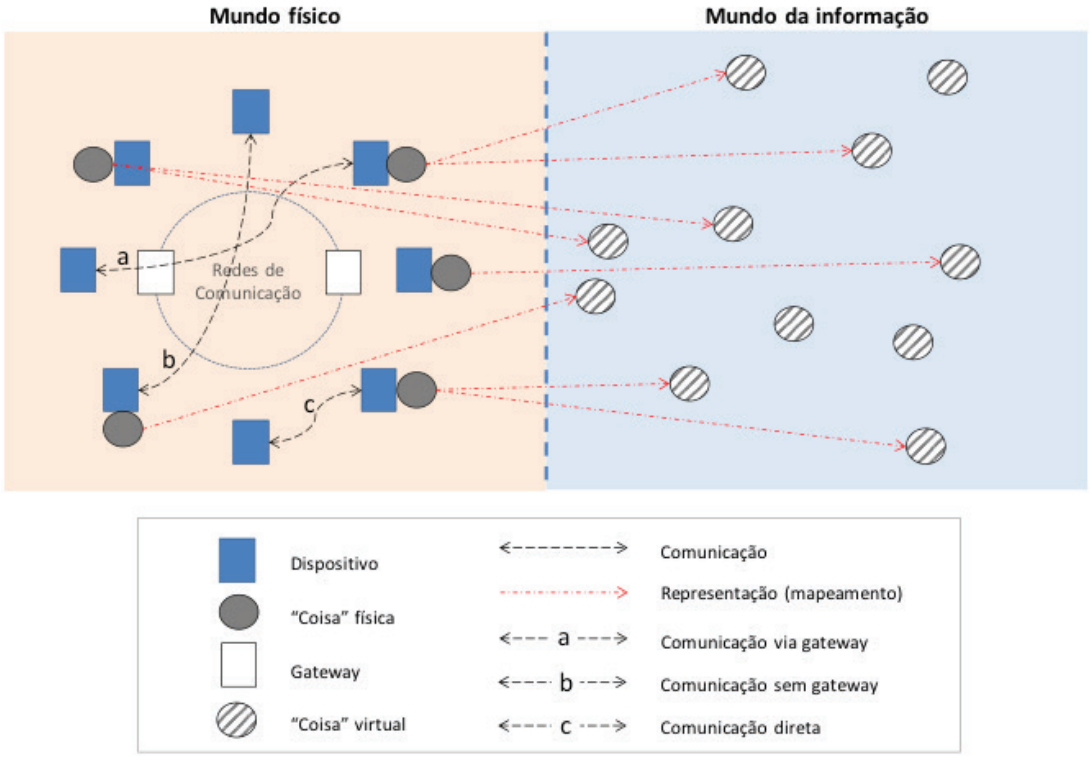
Arquitetura IoT

Por não ser exatamente uma tecnologia, mas sim um novo conceito que abrange várias plataformas, tecnologias e modelos de negócio, a IoT deve estar baseada num consenso[1] entre todas as partes interessadas, para que haja progresso técnico e comercial.

Entre os organismos de *standards*, há definições que estabelecem as bases técnicas da Internet das Coisas. Um dos principais organismos é a ITU (International Telecommunication Union) que estabeleceu essas premissas no seu documento "Recommendation ITU-T Y.2060". (RECOMMENDATION ITU-T Y.2060, 2012).

Uma visão técnica geral da IoT é dada pela ITU e ilustrada na Figura 2.1.

Figura 2.1 – Visão técnica geral da IoT



Fonte: Adaptação de Recommendation ITU-T Y.2060, 2012.

1. Os organismos que desenvolvem *standards* são os responsáveis por estabelecer tal consenso, como visto no capítulo anterior.

Os elementos apresentados nessa ilustração compreendem os diversos dispositivos e tecnologias que fazem parte da IoT e que estão presentes em praticamente todas as definições de organismos e fabricantes. A partir desses elementos, poderemos, adiante, construir uma arquitetura da IoT, e, para isso, é importante compreender cada um desses itens, conforme a ITU. (RECOMMENDATION ITU-T Y.2060, 2012).

Mundo físico e mundo da informação

A IoT pode ser vista como um mundo físico, tendo como paralelo, o mundo digital, da informação, em que existem os elementos virtuais. Cada "coisa" ou objeto do mundo físico pode ser representado no mundo da informação por uma "coisa" virtual[2]; porém, é importante considerar que, no mundo da informação da IoT, podem existir elementos virtuais (coisas virtuais) sem correspondência ao mundo físico. (RECOMMENDATION ITU-T Y.2060, 2012).

Dispositivo

Um dispositivo é o objeto ou equipamento com capacidade mandatória de comunicação e capacidades opcionais de:

- sensoriamento;
- atuação;
- captura de dados;
- memória;
- processamento.

Os dispositivos coletam vários tipos de informações e as encaminham para as redes de comunicação e informação para processamento posterior. Alguns dispositivos podem executar operações com base em informações recebidas das redes de comunicação e informação.

» Dispositivos com representação no mundo da informação são as "coisas" da IoT.

Dispositivos comunicam-se com outros dispositivos, e a capacidade de comunicação é a sua característica mínima para pertencer à IoT.

Podem se comunicar das seguintes formas:

- pela rede de comunicação por meio de gateways (caso "a");
- pela rede de comunicação, sem a utilização de gateways (caso "b"); ou
- diretamente, ou seja, sem passar pela rede de comunicação (caso "c").

Além disso, combinações dos casos "a" e "c" e dos casos "b" e "c" são possíveis. Por exemplo, dispositivos podem se comunicar diretamente por meio de uma rede local (caso "c") e, então, comunicar-se por meio de um gateway da rede de comunicações (caso "a"), ainda conforme Figura 2.1. (RECOMMENDATION ITU-T Y.2060, 2012).

2 Representação do mundo físico no mundo da informação por meio do mapeamento de cada coisa.

Os dispositivos são classificados pela ITU em quatro categorias:

1. Dispositivo de transporte de dados: conectado a um objeto (“coisa física”) para possibilitar a comunicação indireta entre esse objeto e as redes de comunicação.
2. Dispositivo de captura de dados: conectado ao objeto, capaz de ler seus dados e também escrever informações no objeto.
3. Dispositivo sensor/atuador: capaz de detectar e medir informações do ambiente (sensor) e transformar essas informações em sinais digitais, ou, ainda, transformar sinais digitais vindos pelas redes de comunicações em operações (atuador). Muitas vezes, os sensores e atuadores formam redes locais de comunicação cabeadas ou sem fio e interagem com as redes de comunicação por meio de gateways.
4. Dispositivo geral: com capacidade própria de processamento e comunicação, que se comunica diretamente com as redes de comunicação via cabos ou sem fio.

Dispositivos do tipo geral incluem equipamentos diversos no domínio das aplicações IoT, tais como: equipamentos industriais, aparelhos residenciais e telefones celulares/smartphones. Por isso, podem ser também uma composição/conjunto de objetos.

Redes de comunicação

As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para as aplicações e para outros dispositivos, bem como por trazer instruções das aplicações para os dispositivos, de maneira confiável e eficiente, de acordo com a ITU-T. Isso pode ser feito por meio das redes existentes, como TCP/IP, ou por novas gerações de redes de comunicação. (RECOMMENDATION ITU-T Y.2060, 2012).

Ainda que na Figura 2.1 apareçam apenas interações entre dispositivos no mundo físico, há também interações entre coisas no mundo da informação, e entre coisas do mundo físico e do mundo da informação. Além disso, as aplicações da IoT incluem variados tipos de sistemas e plataformas, seja por meio de plataformas proprietárias ou sobre plataformas abertas, com capacidades genéricas, tais como:

- autenticação;
- gestão de dispositivos;
- cobrança;
- contabilidade.

Arquitetura da IoT

A ITU definiu a arquitetura da Internet das Coisas em quatro camadas.

São elas:

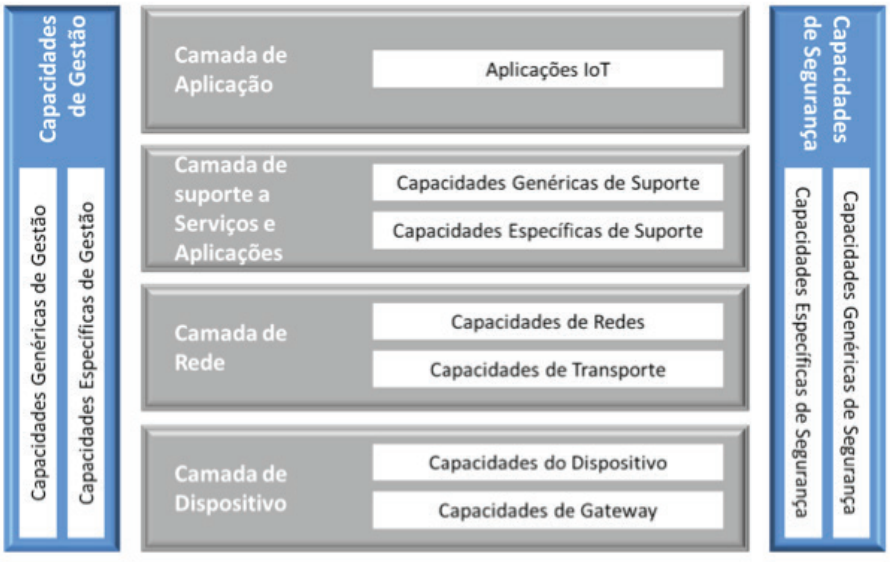
1. Camada de Aplicação.
2. Camada de suporte a Serviços e Aplicações.
3. Camada de Rede.
4. Camada de Dispositivos.

Essas camadas são compreendidas em capacidades de Gestão e de Segurança, que perpassam e garantem a estrutura do todo, ou seja, das quatro camadas. A ITU construiu uma definição de arquitetura que parte do elemento básico da IoT[3], da seguinte maneira:

- na forma como essas coisas interagem por meio de uma rede de comunicações;
- nas aplicações que usam as coisas, recebendo dados e enviando ordens;
- no suporte necessário para essa interação entre as coisas e os sistemas de inteligência (aplicações).

O detalhamento dessas camadas é ilustrado na Figura 2.2:

Figura 2.2 – Arquitetura em camadas da Internet das Coisas



Fonte: Recommendation ITU-T Y.2060, 2012, p. 7.

As aplicações da Internet das Coisas estão na **Camada de Aplicação**.

3. A "coisa" distribuída em ambientes.

Por exemplo: sistemas de medição eletrônica de energia (Smart grid), sistemas de gerenciamento urbano (Smart city), sistemas de automação predial/industrial avançada, monitoramento e gestão da saúde (e-health), modelos de logística e controle de transporte e materiais, entre diversos outros.

Cabe ressaltar que as aplicações na IoT estão, ainda, em fase embrionária de desenvolvimento. De acordo com o desenvolvimento da IoT, inúmeras aplicações surgirão, processo já ocorrido, com o advento da Internet, das redes de telefonia celular, e muitas outras tecnologias disruptivas.

De acordo com o Recommendation ITU-T Y.2060 (2012), a **Camada de suporte a Serviços e Aplicações** é constituída por dois grupos de capacidades de suporte:

1. as Genéricas;
2. as Específicas.

As **Capacidades Genéricas de Suporte** são as funcionalidades comuns, que podem ser usadas por diferentes tipos de aplicações da IoT[4]. Essas capacidades podem ser invocadas por capacidades específicas, quando, por exemplo, no desenvolvimento de novos suportes específicos.

As **Capacidades Específicas de Suporte** são funcionalidades com atribuições particulares, específicas para alguma aplicação na IoT, requisitadas para aplicativos definidos e não gerais. Podem, inclusive, consistir de agrupamentos de capacidades específicas.

De acordo com o Recommendation ITU-T Y.2060 (2012), a **Camada de Rede** é constituída por dois grupos de capacidades, que se referem:

1. às redes de comunicação;
2. ao transporte de dados.

As **Capacidades de Redes** referem-se às funções de controle da conectividade da rede, tais como: funções de controle das fontes de acesso e transporte, gestão da mobilidade ou autenticação, autorização e contabilidade.

As **Capacidades de Transporte** têm foco em prover conectividade para o transporte de dados de aplicações e serviços específicos da IoT, bem como em transporte de informação relacionada à gestão e controle da IoT.

Por fim, a **Camada de Dispositivo** é constituída de dois grupos de capacidades:

1. as relacionadas a dispositivos;
2. as relacionadas a gateways.

4. Tais como: processamento de dados e armazenamento de dados.

Quanto às **Capacidades do Dispositivo**, é importante saber que os dispositivos podem ter diversas funcionalidades, que incluem interação direta com as redes de comunicação (tanto para enviar como para receber informação, sem a necessidade de gateways), e também interação indireta, nesse caso, por meio de gateways. Podem ter, também, a capacidade de criar redes particulares para comunicação em cenários específicos, quando necessário escalabilidade e rápida implantação. Dispositivos podem ter a capacidade de permanecer em estado "dormente", sendo utilizados apenas quando necessário, e, assim, conservar energia.

Quanto às **Capacidades de Gateway**, os gateways devem suportar diversas interfaces e protocolos, realizando a integração entre os dispositivos e a Camada de Rede. Tanto podem suportar tecnologias de interface cabeadas ou sem fio[5], como, na Camada de Rede, integrarem tecnologias de dados em redes 2G/3G, Ethernet, linhas DSL etc. Por sua vez, os gateways devem ter a capacidade de integrar protocolos diferentes, como, por exemplo: o dispositivo em protocolo ZigBee e a Camada de Rede em protocolo 3G.

Capacidades de Gestão

De acordo com o Recommendation ITU-T Y.2060 (2012), as Capacidades de Gestão da IoT compreendem capacidades tradicionais, como: gestão de falha, gestão da configuração, da contabilidade, da performance e da segurança.

Essas capacidades são divididas em dois tipos:

1. genéricas;
2. específicas.

As **capacidades genéricas de gestão** dizem respeito à gestão dos dispositivos, possibilitando ativação e desativação remota, diagnóstico, atualização (upgrade) de *firmware/software*, *status* de funcionamento, gestão da topologia na rede local do dispositivo, gestão do tráfico na rede e aplicação de critérios para serviços críticos.

As **capacidades específicas de gestão** referem-se à gestão dos requisitos específicos das aplicações, como, por exemplo, num sistema de Smart grid, o monitoramento da comunicação em PLC.

Capacidades de Segurança

Conforme o Recommendation ITU-T Y.2060 (2012), as Capacidades de Segurança são classificadas em dois tipos:

1. genéricas;
2. específicas.

5. CANbus, ZigBee, Bluetooth, Wi-Fi.

As **capacidades genéricas de segurança** são capacidades independentes de aplicações, e estão subdivididas em três camadas:

1. Camada de aplicação: referem-se à autorização, autenticação, confidencialidade de dados e proteção da integridade, proteção da privacidade, auditoria da segurança e antivírus;
2. Camada de rede: referem-se à autorização, autenticação, confidencialidade dos dados de uso e de sinalização, e proteção à integridade de sinalização;
3. Camada de dispositivo: capacidades genéricas de autenticação, autorização, validade da integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção à integridade.

As **capacidades específicas de segurança** são aquelas adotadas para aplicações com requisições especiais, tais como: pagamento móvel, aplicações de segurança patrimonial e física etc.

Funcionalidades do objeto – “coisa”

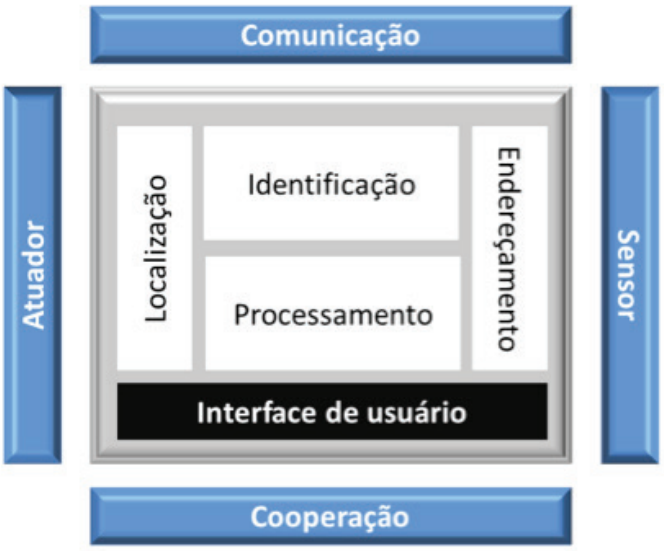
O essencial e que caracteriza a Internet das Coisas são as funcionalidades e atribuições do objeto, da “coisa”, que tanto pode ser um objeto físico quanto virtual, como vimos nas definições da ITU. Isso irá definir o design dos objetos, de aplicações e sistemas e de processos associados à IoT.

São nove as funcionalidades de um objeto na Internet das Coisas, distribuídas em três conjuntos (FACCIONI FILHO, 2016):

1. Conjunto das Características: composto pelas atribuições do próprio objeto;
2. Conjunto das Relações: refere-se a como o objeto interage com outros objetos em rede;
3. Conjunto da Interface: refere-se às relações entre o objeto e o usuário.

A Figura 2.3 apresenta a topologia de funcionalidades da “coisa” na IoT, mas é importante observar que não necessariamente todas as funcionalidades precisam estar presentes em cada objeto, pois dependem do uso de cada objeto e das aplicações IoT em que estão inseridos.

Figura 2.3 – Funcionalidades do Objeto na Internet das Coisas



Fonte: Faccioni Filho, 2016.

No conjunto das **Características**[6], existem as seguintes atribuições do objeto:

- **Processamento**, refere-se à capacidade de processamento computacional inserida no objeto, capaz de fazê-lo agir e responder às requisições da IoT e às suas aplicações;
- **Endereçamento**, refere-se à capacidade do objeto de ser encontrado na IoT, capacidade de ser localizado na rede por meio do roteamento;
- **Identificação**, refere-se à identidade de cada objeto, fazendo-o único em toda a IoT
- **Localização**, relacionado ao local físico em que o objeto se encontra, a sua posição no mapa geográfico.

No conjunto das **Relações**[7], que se referem às capacidades de interação da "coisa" com outros objetos (físicos ou virtuais) na rede, existem as seguintes funcionalidades:

- **Comunicação**, capacidade do objeto de receber e/ou enviar mensagens para outros objetos na rede IoT;
- **Cooperação**, capacidade do objeto de agir em comum com outros objetos, visando a atividades e aplicações cooperadas, ou seja, ações conjuntas e de colaboração;
- **Sensoriamento**, capacidade do objeto de captar dados do ambiente ou de outros objetos, dados obtidos por meio de sensores presentes no próprio objeto e que permitem monitorar determinadas grandezas do ambiente;
- **Atuação**, capacidade do objeto de agir sobre o ambiente, operando e modificando a condição de um determinado meio.

6. Identificado pelos retângulos brancos na Figura 2.3.

7. Identificado pelos retângulos azuis na Figura 2.3.

O conjunto da **Interface**[8] se refere à interação do objeto com o usuário, permitindo-lhe visualizar informações do objeto, realizar configurações e modificar sua condição.

Compreendendo todas essas características do objeto, e da arquitetura da IoT, pode-se desenvolver aplicações específicas. Essas aplicações guardam características técnicas e funcionalidades únicas, não encontráveis em outros sistemas ou mesmo na internet, como a conhecemos hoje. O desenvolvimento de soluções específicas para a Internet das Coisas demanda uma visão de design de produto e de aplicações, que se configura como plataforma, ou sistema. Assim, antes de analisarmos algumas aplicações já correntes na IoT, é importante uma visão do processo de criação e desenvolvimento desses produtos.

Desenvolvimento de soluções IoT

Os desafios colocados pela Internet das Coisas, no processo de *design*, podem ser percebidos pela quantidade de soluções imaginadas e algumas já existentes ou em preparação.

? Como o *design* está se articulando para esses desafios de criação?

Conforme Chimero (2012) e Faccioni Filho (2016), o *design* de um objeto ou solução para a IoT pode ser encarado como uma relação entre três forças em torno de uma ideia:

1. **Compreensão** da ideia do objeto/solução, que está relacionada com o entendimento profundo e variado do que virá a ser a ideia quando materializada no resultado;
2. **Explicação** da ideia do objeto/solução, que é feita nas tentativas de explicar os detalhes da ideia, dialogar com a própria ideia na esperança de clareá-la;
3. **Expressão** da ideia do objeto/solução, que é a concepção formalizada, ou antecipação do objeto em seu modelo, com “algo” para apresentar, de um determinado “jeito” e com uma “forma”.

No *design*, procuramos copiar (observar) a natureza no que diz respeito às suas funcionalidades, e também em seu desenho, e, a partir disso, transformar cópias em funcionalidades (COSTA, 2014), sejam novas funcionalidades ou aprimoramentos.

8. Identificado pelo retângulo preto na Figura 2.3.

De acordo com Faccioni (2016), o processo para aprimorar uma ideia, objeto ou sistema passa por exercícios contínuos de:

- **Simplificação**, em que cada novo desenho é repensado no sentido de simplificar o desenho prévio;
- **Limpeza**, ao retirar os excessos e redundâncias, retirar o que não é necessário;
- **Redução**, em que a ideia nova tem menos partes, menos peças, menos controles, menos intermediários do que a ideia anterior;
- **Unificação**, quando o aprimoramento busca juntar partes, juntar modelos, sintetizar;
- **Consolidação**, para então fixar e dar um sentido único e estável à ideia, chegando a um objeto minimamente viável.

Nesse processo de design, a imaginação (criação de imagens) move-se das ideias para os projetos, e os projetos são as tentativas de materializar as ideias. Esse movimento, no entanto, é pendular, pois os projetos dão origem a novas ideias, que serão capazes de modificar e melhorar os projetos anteriores, e assim por diante, num pêndulo de criação.

Ferramenta essencial, então, é a criação de modelos.

Modelos para expressar as ideias do projeto fazem com que se estabeleçam limites, restrições, e, dentro desses limites, há uma concentração, a qual permite um *design*.

O modelo parte de um desenho intuitivo, é uma visão genérica que define um espaço, e, então, persegue-se um conteúdo real que o preencha: uma fórmula, um volume, um objeto.

A intuição funciona como o caminho de mão dupla entre a ideia e o projeto, e o movimento pendular do design (ideia <-> projeto) nada mais é do que a oscilação da intuição entre os diversos polos da criação do objeto:

- como é o projeto e porque ele existe;
- o objeto visto de muito perto e de muito longe;
- pensar no objeto e materializar o objeto;
- o objeto na sua característica mais simples e operacional, e seu caráter de estratégia e de visão geral;
- moldar uma versão do objeto e analisar, para então buscar uma nova versão.

Esses polos da criação de objetos, sejam eles “coisas” físicas ou virtuais na Internet das Coisas, estão ilustrados na Tabela 2.1, em que vemos as diversas oscilações do *design*:

Tabela 2.1 – Oscilações do movimento pendular do *design*

Oscilações – a criação no design	
Como?	Por quê?
Próximo	Distante
Fazer	Pensar
Operacional	Estratégico
Moldar	Analisar

Fonte: Faccioni Filho, 2016.

Dessas oscilações da criação, surgem aplicações variadas da comunicação entre máquinas (M2M), da telemetria, dos objetos para "vestir" (Wearables), da computação aplicada à IoT (Fog Computing), das aplicações como Smart Grid, Smart Cities, Automação Predial e muitos outros, como se verá adiante.

Referências

CHIMERO, Frank. **The Shape of Design**. Minnesota: Shapco Printing, 2012.

COSTA, Luís Alves. **Da Geometria à Estética, através das formas naturais**. Vila Nova de Famalicão, Portugal: Edições Húmus, 2014.

FACCIONI FILHO, Mauro. Designing "things" for the Internet of Things. In: I **CONGRESSO INTERNACIONAL, I; WORKSHOP DESIGN & MATERIAIS**, VII, 2016, São Paulo: Universidade Anhembi Morumbi, 2016.

RECOMMENDATION ITU-T Y.2060. **Overview of the Internet of things**. ITU-T – International Telecommunication Union, 2012.

Capítulo 3

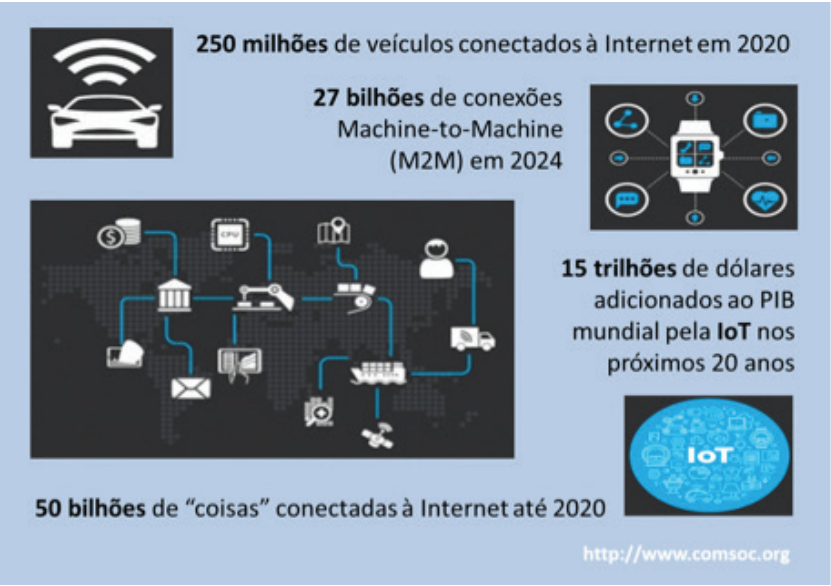
Aplicações de mercado

Mercado atual e tendências

A Internet das Coisas já é uma realidade e está avançando silenciosamente para todas as esferas do nosso cotidiano: desde a comunicação da internet com veículos (e entre veículos) até os sistemas de saúde com monitoramento *on-line* de pacientes, passando por medição eletrônica de consumo de energia e controle do gado em campo. Os principais institutos mundiais de pesquisa e de desenvolvimento tecnológico estão constantemente avaliando essas tendências e aprimorando seus relatórios.

Um dos mais importantes e reconhecidos desses órgãos é o **IEEE – Institute of Electrical and Electronic Engineers**, que tem sido, por décadas, o responsável pelas principais normas relacionadas às novas tecnologias. Entre suas diversas sociedades, a IEEE Communications Society – ComSoc – tem se dedicado a estudar os caminhos da IoT. De acordo com a IEEE Communications Society (COMSOC, 2015), em 2020 cerca de 250 milhões de veículos estarão conectados à internet para os mais diversos serviços e aplicações[1]. Conexões diretas entre máquinas (Machine-to-Machine – M2M) alcançarão 24 bilhões de conexões anuais, por volta de 2024. A previsão é de que, em 2020, cerca de 50 bilhões de "coisas" estarão conectadas à IoT, e nos próximos 20 anos, a Internet das Coisas acrescentará 15 trilhões de dólares ao PIB mundial (Produto Interno Bruto). A Figura 3.1 ilustra essas previsões:

Figura 3.1 – Tendência da IoT de acordo com o IEEE Communications Society



Fonte: Adaptação de ComSoc, 2015.

1. Tais como: controle de tráfego, prevenção a acidentes, relatórios online para mecânica e manutenção, entre diversas outras possibilidades

De acordo com a organização **Business Insider**, no artigo de Greenough e Camhi (2016), considera-se que a Internet das Coisas é a próxima revolução industrial, pois será a forma com que empresas, governos e indivíduos vão interagir com as coisas do mundo físico. Nesse trabalho da Business Insider, os seguintes pontos-chave são apresentados:

- projeção de 34 bilhões de dispositivos conectados à internet em 2020;
- desses, 24 bilhões serão dispositivos específicos da IoT, e 10 bilhões serão equipamentos tradicionais[2];
- nos próximos cinco anos, serão gastos 6 trilhões de dólares com soluções IoT;
- os principais usuários de soluções IoT serão as empresas, considerando as seguintes vantagens que a IoT propicia: redução de custos operacionais, maior produtividade, expansão para novos mercados ou novos produtos;
- o segundo maior usuário da IoT provavelmente será o governo, com foco em maior produtividade, menores custos e melhoria da qualidade de vida dos cidadãos;
- em terceiro lugar, estarão os consumidores, adotando funções da IoT de uso pessoal, mesmo assim com enormes montantes de dinheiro investidos.

Ahmed Banafa (2015), em seu artigo “Internet of Things (IoT): Security, Privacy and Safety”, discute vários aspectos da Internet das Coisas com relação à privacidade e segurança, e também sobre suas tendências de evolução e impactos na sociedade. Ele considera a IoT como sendo a terceira onda no desenvolvimento da Internet:

1. a **primeira onda**, nos anos 1990, trouxe para a internet cerca de 1 bilhão de usuários;
2. a **segunda onda**, nos anos 2000, trouxe mais 2 bilhões, por meio do acesso via celulares;
3. a IoT (a **terceira onda**) deverá conectar cerca de 28 bilhões de “coisas” por volta de 2020, desde carros até braceletes e acessórios pessoais.

Com isso, uma tendência deverá ganhar grande reforço: esses bilhões de dispositivos representarão bilhões de oportunidades para acessos indevidos, insegurança e invasão de privacidade. Banafa (2015) cita estudos da Cisco Systems que consideram que a IoT deverá gerar ganhos de mais de 19 trilhões de dólares para as empresas até 2020, e que o instituto IDC projeta ganhos de 8,9 trilhões de dólares em serviços e tecnologias IoT até o final desta década.

Segundo a ISOC – Internet Society (ROSE; ELDRIDGE; CHAPIN, 2015), várias empresas estão pesquisando e analisando as projeções da IoT no mercado mundial, como, por exemplo, a Morgan Stanley, que prevê 75 bilhões de dispositivos conectados em 2020; enquanto a Huawey projeta um número de 100 bilhões de conexões à IoT em 2025. Cita o Instituto Mackinsey Global, que sugere um impacto financeiro que varia de 3,9 a 11,1 trilhões de dólares na economia global em 2025.

2. Como: smartphones, tablets, relógios inteligentes etc.

A ISOC considera várias tendências de aplicações para as soluções IoT, de acordo com cenários específicos, ilustradas no Quadro 3.1.

Quadro 3.1 – Tendências de aplicações IoT conforme cenários

Cenários para aplicações IoT		
Cenário	**Descrição**	**Exemplos**
Seres humanos	Dispositivos "vestidos" ou dentro do corpo humano	Relógios, monitores de batimento cardíaco, sensores de temperatura, pressão, marca-passo, segurança, etc.
Residências	Edificação de moradia e convivência	Sistemas de segurança, automação predial, controles diversos.
Ambientes comerciais	Espaços em que há negócios, comércio, vendas	Lojas, bancos, restaurantes, estádios, pontos de venda, mercados, etc.
Escritórios	Espaços de trabalho administrativo / intelectual	Gestão de energia, de segurança, de telecomunicações
Indústrias	Ambientes fabris e de exploração	Locais de trabalho rotineiro, padronizado, o que inclui hospitais, fazendas, e também minas, exploração de gás e petróleo, visando produtividade
Transportes	Sistemas embutidos em veículos	Carros, trens, navios, caminhões, aviões, visando monitoramento e melhoria de uso.
Cidades	Ambientes urbanos	Espaços públicos, infraestrutura, smart meters, monitoramento ambiental
Rural	Ambientes fora das áreas urbanas	Monitoramento de espaços abertos, clima, sistemas de transporte aéreo, geolocalização.

Fonte: Adaptação de Rose, Eldridge, Chapin, 2015.

Como se vê, não importa qual instituto, empresa ou organização, todos projetam números gigantescos, seja de dispositivos conectados ou de valores econômicos. É uma revolução, em todos os aspectos.

? Mas quais seriam tais soluções e produtos? O que está acontecendo, agora?

Vejamos, a seguir, alguns casos - como M2M, veículos, vestíveis, Smart grid, tecnologia de Fog computing - e algumas outras soluções já em uso.

M2M – Machine-to-Machine

Como vimos no capítulo inicial, a denominação "M2M – Machine-to-Machine" refere-se à "comunicação entre duas ou mais entidades que não necessariamente precisam da intervenção humana para ocorrer; serviços M2M devem automatizar processos de decisão e comunicação." (MINERVA, 2015, p. 12). Essa definição partiu da ETSI e, muitas vezes, a M2M confunde-se com a IoT.

» Apesar de o mercado manter a sigla M2M, é provável que, com o tempo, venha a diluir-se dentro da própria Internet das Coisas, caracterizando apenas as aplicações entre máquinas e sem intervenção humana.

A M2M tem tido uma grande expansão, pois inúmeras aplicações têm esses atributos de plataforma em que atuam exclusivamente dispositivos com comunicação sem fio. Um relatório preparado pelas organizações Machine Research e Aegis Systems (AEGIS, 2014) analisa o mercado M2M e divide

suas aplicações em 12 segmentos, ou setores, de mercado. Essa análise apresenta diversas aplicações específicas e demonstra a força do desenvolvimento tecnológico e econômico da M2M.

Segundo o relatório da Aegis (2014), os setores do mercado e as correspondentes aplicações M2M, divididas em grupos e apresentadas como as de maior impacto, são:

Quadro 3.2 – Mercado e aplicações M2M

Setor do mercado	Aplicações M2M
Agricultura e Meio Ambiente	Monitoramento ambiental. Pesca: pesca em águas profundas, na costa e fazendas de criação. Agricultura: equipamentos agrícolas, gestão de colheitas, gestão de estoques. Novas fontes de energia.
Automotivo	Chamadas de emergência, internet e entretenimento, seguro automotivo, locação de veículos, dados de fabricação, navegação, segurança, assistência e recuperação de veículos, serviços de voz.
Construção	Monitoramento de equipamentos, inventários, desgaste. Visualização on site: projetos on-line, óculos de realidade aumentada, visão 3D. Monitoramento de site: alarmes, CFTV.
Eletrônica de consumo	Displays: projetores, telas, televisores. Fontes audiovisuais: fontes de áudio, controles, consoles de games, fontes de vídeo. Dispositivos domésticos: telas distribuídas, equipamentos de internet, expositores de imagens, dispositivos de etiquetagem RFID. Equipamentos de rede: memória de rede, impressão, digitalização, telefones VOIP, webcam. Outros: fitness, estações de meteorologia. Multimídia pessoal: câmera, console de game, áudio player, óculos de vídeo, vídeo player. Aplicações de localização: crianças, animais domésticos. Cozinha: lavadoras e secadores de louça, geladeiras, congeladores, fogão, acessórios.
Serviços de Emergência e Segurança	Defesa: pessoal, infraestrutura e equipamentos, armas inteligentes. Serviços de Emergência: emergência médica, bombeiros, dispositivos contra incêndio, polícia. Segurança Nacional: controle de fronteira, penitenciárias, guardas, gestão de locais públicos.

Saúde	Assistência à vida: alarmes de soluções de assistência, soluções abrangentes de suporte, distribuição de medicamentos, localização de pessoas, ambientes de apoio clínico. Monitoramento clínico remoto: cardíaco, diabetes. Exames clínicos: monitoramento de exames e testes clínicos. Sistemas médicos interligados: acompanhamento e rastreamento hospitalar, acompanhamento e rastreamento de fornecedores. Conectividade a sistemas de socorro: soluções para ambulâncias e outros atendentes de emergência. Telemedicina: local e móvel. Monitoramento do bem-estar: treinamento/fitness, controle de peso. Equipamentos de bem-estar: soluções multidispositivos, soluções multifunções.
Prédios Inteligentes	Microgeração: cogeração residencial/empresarial, fonte geotérmica residencial/empresarial, energia solar residencial/empresarial, energia eólica residencial/empresarial. Segurança: alarmes, controle de acesso, CFTV, alarmes de incêndio, intercomunicadores. Automação predial: painéis de controle, dispositivos de controle remoto, ar condicionado, gestão de energia, iluminação. Infraestrutura de Rede: tecnologias alternativas, modens, roteadores, switches e outros dispositivos de rede.
Indústria e Fornecedores	Extração: carvão, óleo, gás, minerais. Manufatura/processamento: diagnóstico remoto e manutenção, monitoramento, controle. Distribuição e transporte: rastreamento de ativos e monitoramento, gestão de frotas - rodoviário, ferroviário, marítimo, oleodutos, aviões de carga. Máquinas de venda/dispensa automática. Armazenagem/estoque: gestão de inventário, monitoramento.
Varejo e Lazer	Controle de acesso: lojas, parques, mercados, centro esportivo, monitoramento. Aplicações de consumo: equipamento audiovisual, fitness, equipamentos de cozinha. Pagamento: caixas registradoras, terminais NFC, estações de pagamento, posição de vendas. Aplicações específicas: terminais de autoatendimento, máquinas de jogo, pontos de informação.

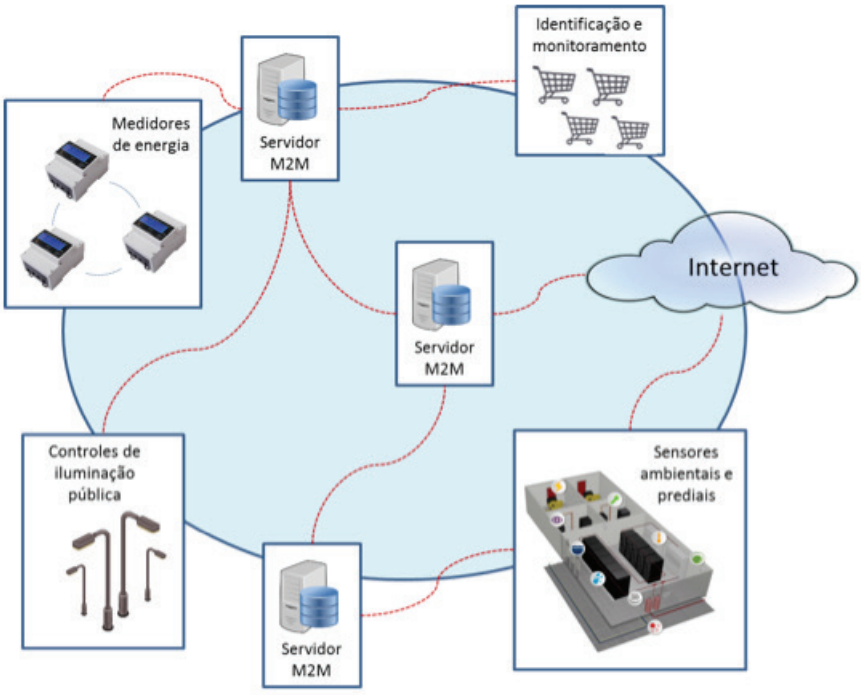
Cidades e Tráfego Inteligente (Smart Cities)	Segurança pública e ambiental: alarmes, CFTV, cultura/turismo, iluminação pública, intercomunicadores. Anúncios em espaço público: área de tráfego, anúncios estáticos. Transporte público: aéreo, ferroviário, rodoviário, naval, emissões de bilhetes, informação a passageiros. Gestão do tráfego: infraestrutura de pedágio, cobranças, sinalização interligada, câmeras e radar, dispositivos embutidos em veículos, pagamento de estacionamento, gestão de espaço em estacionamento, iluminação de estrada/rua, monitoramento de congestionamento e volume de tráfego.
Gestão Empresarial	Equipamentos de escritório convencionais. Equipamentos específicos.
Concessionárias/ Utilities	Carga em veículos elétricos. Medição eletrônica inteligente: eletricidade, gás, água. Gestão da distribuição: eletricidade, gás, água.

Fonte: Aegis, 2014.

Por essa longa série de aplicações M2M e seu evidente paralelo com a própria Internet das Coisas, pode-se perceber o potencial de tecnologias e negócios envolvidos.

A Figura 3.2 ilustra diversos componentes presentes na M2M, com aplicações típicas e seus respectivos mercados.

Figura 3.2 – Visão geral de aplicações e mercado M2M



Fonte: Elaboração do autor, 2016.

Telemetria

A telemetria refere-se à coleta de dados em campo e, com isso, a medição, controle e comunicação desses dados até centrais em que os dados são analisados e parametrizados. Utiliza interfaces em campo[3], convertendo os dados coletados em sinais digitais para transmissão por meios disponíveis[4]. A centralização dessas informações permite o monitoramento dos dados para avaliações, análises diversas, atuação, gestão e controle.

A telemetria está na origem da Internet das Coisas, como vimos no desenvolvimento da RFID. A demanda por telemetria está se expandindo para as mais diversas áreas, e confunde-se com alguns dos setores descritos anteriormente ao nos referirmos ao M2M, porém, a telemetria pode ser considerada apenas como umas das aplicações da M2M. Destaca-se nos seguintes setores:

- Concessionárias de energia: medição eletrônica de tensão, corrente, consumo, permitindo monitoramento remoto dos consumidores, bem como verificação da qualidade de energia e condições operacionais;
- Concessionárias de água: medição eletrônica de consumo, permitindo monitoramento remoto dos consumidores, bem como verificação da qualidade de água (e esgoto) e condições operacionais;
- Concessionárias de gás: medição eletrônica de consumo, permitindo monitoramento remoto dos consumidores, bem como condições operacionais da infraestrutura;
- Veículos: sensoriamento dos itens operacionais do veículo, permitindo tanto o monitoramento por parte do condutor, como pelo fabricante e equipes de manutenção remota/mecânicas;
- Aviões: sensoriamento dos itens operacionais do avião, sensoriamento das condições externas, entre outros itens, permitindo o monitoramento em tempo real por equipes de pilotagem e equipes remotas (em terra); o mesmo se aplica a espaçonaves e satélites;
- Meteorologia e Ambiental: monitoramento das condições meteorológicas em pontos diversos, permitindo avaliações precisas e distribuídas em áreas geográficas estratégicas[5];
- Medicina: monitoramento de ambientes clínicos, monitoramento de testes em tempo real;
- Agricultura: monitoramento de grandezas de impacto na agricultura[6],

A telemetria tem sido usada há algum tempo, e é anterior à Internet das Coisas. Porém, devido à sua aderência ao conceito de IoT e capacidade de ampliar seu uso com os atributos da Internet, é um fator de sucesso e oportunidade de mercado.

3. Tais como: sensores de temperatura, umidade, voltagem, corrente e inúmeros outros,

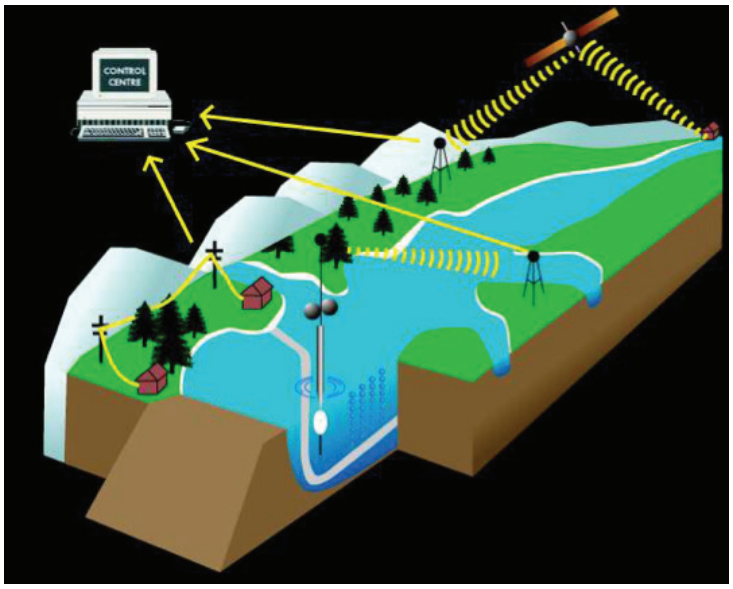
4. Tais como: redes sem fio (RF, GPRS/2G/3G, ZigBee etc.) e/ou redes cabeadas (metálicas e ópticas).

5. Temperatura, umidade, pressão, vento, luminosidade, vibrações etc.

6. Tais como: temperatura, umidade, solo etc.

Na Figura 3.3, pode-se ver uma ilustração de aplicação de telemetria da empresa Trans Communications, como um exemplo típico em que dados são obtidos em áreas diversas, transmitidos por cabos e por fios numa situação híbrida, até a central de controle.

Figura 3.3 – Exemplo de aplicação de telemetria



Fonte: Trans Communications, 201?.

Wearables (vestíveis)

O termo *wearables*, que pode ser traduzido por vestíveis, refere-se às tecnologias que são incorporadas a roupas e a outros acessórios que usamos diariamente para nos vestir, praticar esportes, enfeitar e proteger do tempo. A Internet das Coisas popularizou-se a partir desses produtos, pois os usuários comuns passaram a ter contato com relógios e óculos que podem acessar a internet, enviar e trazer informações, entre muitas outras aplicações, e, com isso, houve um entendimento imediato do potencial desses pequenos dispositivos incorporados em "vestíveis" e suas interações com a grande rede.

Aplicações que exigem conectividade e que precisam estar junto de cada pessoa são as que tiram proveito de relógios de pulso, roupas, celulares, tênis, óculos, joias etc.

> Rastreamento de atividades físicas é um exemplo típico: corrida e bicicleta utilizam esses aplicativos para medir o ritmo do treino, elevações da pista, intervalos, mapa, batimentos cardíacos, entre outras informações, e incorporam alarmes, avisos, trabalho em equipe e várias outras possibilidades.

Os aplicativos necessitam de dispositivos minúsculos com capacidade de processamento e conectividade, que podem estar em um ou em mais de um conjunto de produtos[7].

7. Tais como: relógios, celulares, processadores em tênis e sapatilhas, bonés, óculos, camiseta.

De maneira muito similar às atividades físicas, existem aplicações focadas em saúde. Parâmetros como pressão, temperatura corporal e batimento cardíaco podem ser constantemente monitorados, por meio de *wearables*, e enviados para centros clínicos remotos. A resposta médica passa a ser virtualmente imediata, com análises preventivas e opções de ação antes impossíveis.

De acordo com Richmond (2013), os vestíveis poderão ser muito mais do que apenas processadores ou cartões inteligentes embutidos ou acoplados em dispositivos comuns e roupas. As roupas poderão ser inteligentes, com aproveitamento da própria tessitura de fios e nanotecnologias para criar sistemas de processamento e, assim, poderão mudar de cor, regular a temperatura do corpo, incorporar *gadgets* e aplicativos em sua estrutura própria de memória. Até mesmo dispositivos implantados no corpo farão parte dessas possibilidades: basta lembrar que isso já é uma prática médica, como, por exemplo, marca-passos e implantes cocleares.

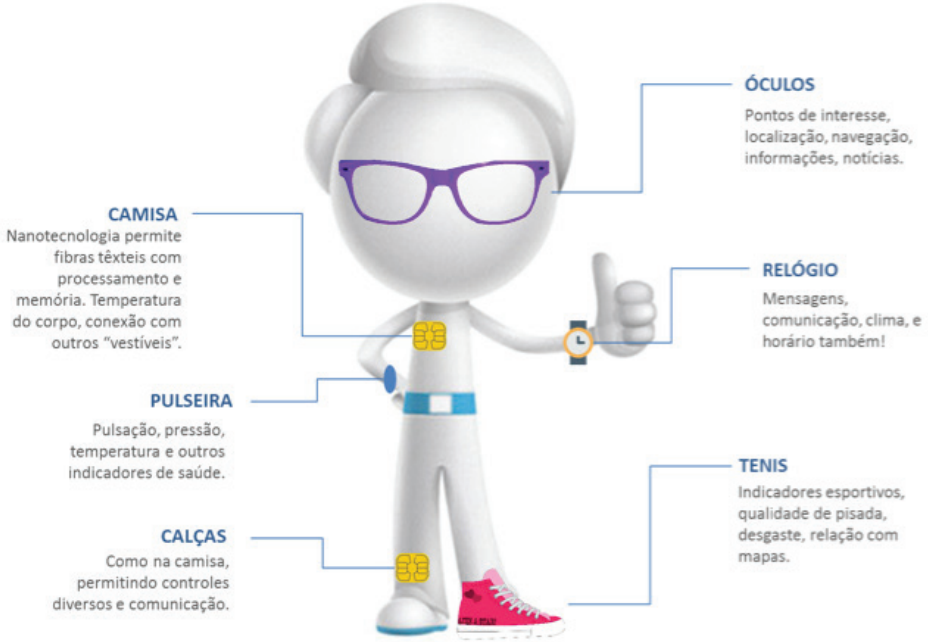
Mas há muita controvérsia a respeito dos *wearables*, seja de fundo médico, seja de fundo ético, comercial ou de segurança e privacidade. Tantas informações pessoais disponíveis na Internet das Coisas poderão ser usadas de forma não esperada ou desejada.

» Por exemplo, sobre o estilo de vida ou condições físicas de cada pessoa, em que isso poderia impactar na aceitação em um novo emprego?

De qualquer forma, a tecnologia continua seus avanços, a despeito das discussões de possibilidades de uso ou de como os consumidores se comportarão.

Na Figura 3.4, alguns exemplos típicos de *wearables* ilustram as aplicações da IoT no contexto de cada indivíduo.

Figura 3.4 – Tecnologias “vestíveis” da Internet das Coisas



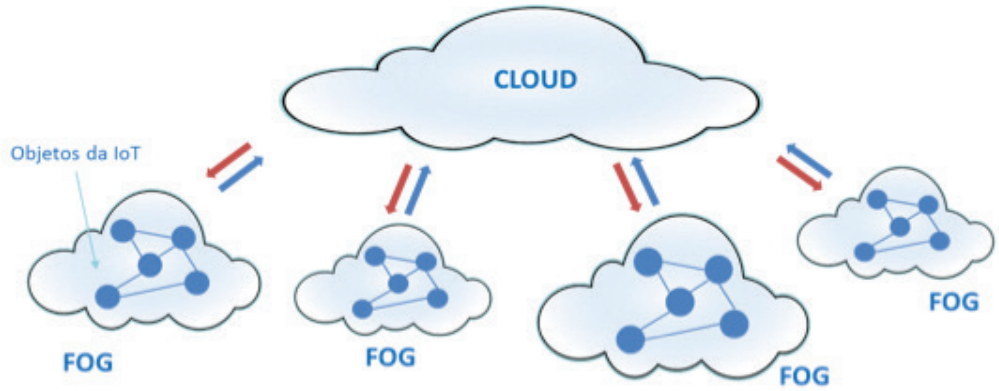
Fonte: Elaboração do autor, 2016.

Fog Computing

Já estamos acostumados a ver a internet representada como uma "nuvem" em desenhos, diagramas e ilustrações, em geral. O tema da computação em nuvem, ou *Cloud*, em inglês, já é recorrente e nos leva à imagem de que as aplicações e os bancos de dados não estão localizados em computadores ou servidores locais, mas sim em ambientes distribuídos, ou seja, em *data centers* espalhados ao redor do mundo. Dessa forma, não sabemos exatamente em que local um processo está sendo computado, pois pode estar acontecendo em locais diferentes e com processos em paralelo. A imagem da nuvem nos leva também a pensar em algo distante, no "céu", longe do nosso alcance.

A internet das coisas traz uma imagem diferente, pois entendemos as coisas como objetos próximos de nós, tais como os sensores, os vestíveis, os dispositivos básicos das residências. Essa noção de proximidade das coisas e a amplidão sugerida pela IoT inspiraram um outro modelo de computação, mais próximo de cada um de nós. E esse modelo, contrapondo-se à nuvem distante, é o da "névoa/neblina", ou *fog*, em inglês, como se pode compreender na ilustração da Figura 3.5.

Figura 3.5 – Computação em nuvem (Cloud) e em névoa (Fog)



Fonte: Elaboração do autor, 2016.

Na *Fog*, ao contrário da *Cloud*, a computação está distribuída entre os componentes da IoT, ou localizada em dispositivos próprios e que se relacionam diretamente com os objetos, sem a necessidade de conexões com bancos de dados ou aplicações na nuvem. Essa noção é profundamente coerente com a IoT, pois cada vez mais se considera que as coisas precisam incorporar funcionalidades relacionadas a processamento (que implica em "inteligência"), comunicação e armazenamento de informações no próprio objeto.

De acordo com Allen (2014), a discussão entre processamento centralizado e distribuído ainda não é comum nos círculos de debates sobre IoT, pois o modelo típico ainda é o de considerar que as "coisas" irão se reportar aos processos na *Cloud*. Mas o impacto crescente do volume de dados na rede está exigindo uma reconsideração sobre esse ponto, e a Cisco está na liderança dessa discussão, pois já prevê volumes excessivos de dados circulando na rede e "subindo" até a nuvem, o que pode ser um contrassenso, especialmente quando é perfeitamente possível a um processo de baixo nível ser realizado e resolvido localmente – basta haver inteligência local para isso.

O conceito de *Fog Computing* foi lançado pela Cisco como uma iniciativa para levar a empresa para a fronteira de inteligência da internet, e para isso desenvolve, também, um sistema operacional aberto e capaz de rodar em seus roteadores e *switches*, bem como em equipamentos de terceiros. O foco é distribuir a massiva quantidade de dados e processos para a periferia da rede, ou seja, para a névoa, e apenas anomalias ou processos específicos para a nuvem.

Fog não é um novo acrônimo na área de tecnologia, mas um conceito que literalmente quer dizer que a "nuvem" está próxima do "chão" para a Internet das Coisas. (ALLEN, 2014). A *Fog* é uma camada intermediária entre o objeto e a nuvem, permitindo distribuir inteligência dentro da rede e, assim, habilitar os desenvolvedores para a criação de soluções IoT diretamente junto aos objetos e suas relações próximas. É uma camada de inovação que aponta para o foco exato da IoT: a inteligência das "coisas" no seu próprio ambiente.

Smart Grid

Smart Grid é a expressão que se popularizou em todo o mundo como sinônimo de redes de distribuição elétrica inteligentes. Com o advento da Internet das Coisas, o *Smart Grid* imediatamente passou a ser um dos seus campos de aplicação mais importantes, ao lado das *Smart Cities* e de outros sistemas de uso público caracterizados como *Smart*, ou inteligentes.

O desenvolvimento do *Smart Grid* está associado a vários direcionamentos de eficiência energética em todo o mundo. Nos Estados Unidos, o departamento nacional de energia criou uma unidade especial denominado *SmartGrid,* justamente para reunir estudos e experiências sobre o tema, bem como divulgar resultados e boas prática.

A internet das coisas está no centro desse novo processo devido à sua capacidade de telemetria avançada, associada à comunicação de dados e a variados tipos de tecnologias.

Na expressão, o *grid* se refere à malha de distribuição de energia elétrica, em que há uma rede de medidores junto aos consumidores, bem como distribuição elétrica de baixa, média e alta tensão, subestações, transformadores e diversos outros componentes, desde a geração da energia até o seu consumo final. Essa rede tem um modelo técnico centenário, e para que fique *smart*, é necessário introduzir as novas tecnologias digitais ao seu contexto. Isso quer dizer que a *grid* será *smart* quando pudermos automatizar os diversos componentes, introduzindo sensores para monitoramento da distribuição, medidores de energia computadorizados, sistemas de comunicação para controle em tempo real, e tudo isso operando de forma integrada. Sistemas computacionais devem agregar algoritmos de simulação, análise e previsão de riscos, com capacidade de atuação.

Os principais benefícios associados ao *Smart Grid*, de acordo com os estudos, experiências e expectativas da área, são:

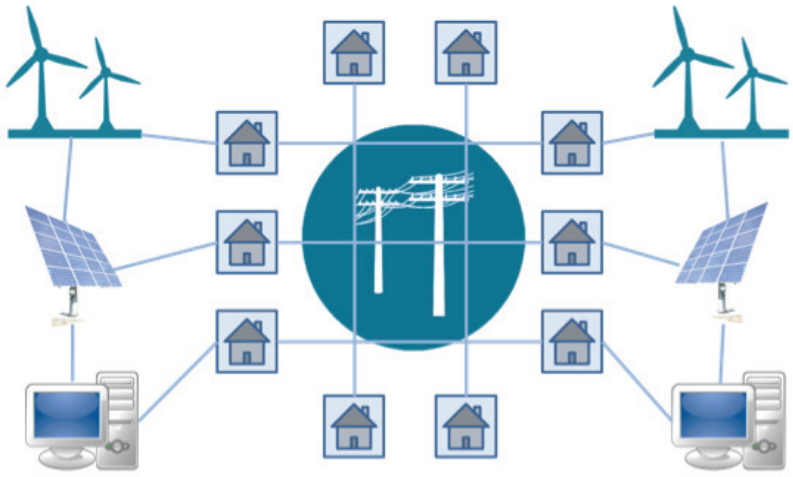
- melhoria da qualidade de energia;
- mais eficiência na transmissão e distribuição de energia;
- medição eletrônica do consumo em cada residência;
- capacidade de restaurar rapidamente a rede elétrica, com ganhos em resiliência;

- redução geral de custos de operação e manutenção;
- redução de preços para o consumidor;
- integração de sistemas de energia renovável de todos os portes à rede elétrica, incluindo microgeração;
- melhoria de segurança;
- capacidade de visão da rede numa estrutura macro, permitindo análises de rede automatizadas;
- medição da energia em sentido duplo, ou seja, tanto do que é utilizado pelo consumidor final quanto do que é produzido por ele, permitindo precisão das faturas (débitos/créditos de energia);
- atribuição, ao consumidor final, do acesso ao seu próprio consumo, em tempo real, permitindo controle local e planejamento individual de demandas.

Um dos componentes do *smart grid* que oferece maior visibilidade à IoT é o *smart meter*, ou medidor eletrônico inteligente. Como uma "coisa" da IoT, o antigo medidor de cada uma de nossas casas passa a ser um componente eletrônico que coleta dados, faz processamento local e envia para centrais de controle e medição as informações, usando redes locais cabeadas ou sem fio, construindo pequenas estruturas de dados locais/regionais, como "fogs", ou mesmo enviando para a nuvem. O comportamento de "coisa inteligente" faz do antigo medidor um "medidor inteligente".

Na Figura 3.6 vemos ilustração do *smart grid* como a composição de diferentes medidores, sensores e sistemas de geração e distribuição, com soluções de comunicação e processamento que estruturam um sistema inteligente.

Figura 3.6 – *Smart grid*



Fonte: Elaboração do autor, 2016.

Como podemos ver, dispositivos IoT estão em todas as partes dessa rede, e se comunicando com outros sistemas, como os de cidades inteligentes (*smart cities*), segurança pública (com monitoramento de incêndios e desastres), saúde ambiental, jogos, lazer e muitos outros que podem ser agregados, dependendo apenas de investimento e criatividade.

Automação Predial – estudo de caso

Um dos mais promissores usos da IoT está na automação predial e residencial. De acordo com Faccioni Filho (2015), há uma nova geração de sistemas de automação e gestão predial, e isso se deve à chegada e expansão da Internet das Coisas.

A automação predial e residencial já é algo corrente, e podemos lembrar de itens como os sistemas de controle de acesso, circuito fechado de televisão, automação da iluminação, sensores de presença, irrigação automática, controle de estacionamento, cortinas automáticas, e muitas outras soluções. Porém, esses produtos, em sua maioria, até o momento, não contêm as funcionalidades que caracterizam um objeto da IoT, de acordo com o que vimos no capítulo 2. Processamento interno e memória local são atributos que não estão na maioria dos sensores atuais do mercado. Ao mesmo tempo, não há um *design* de produtos e soluções com foco em IoT.

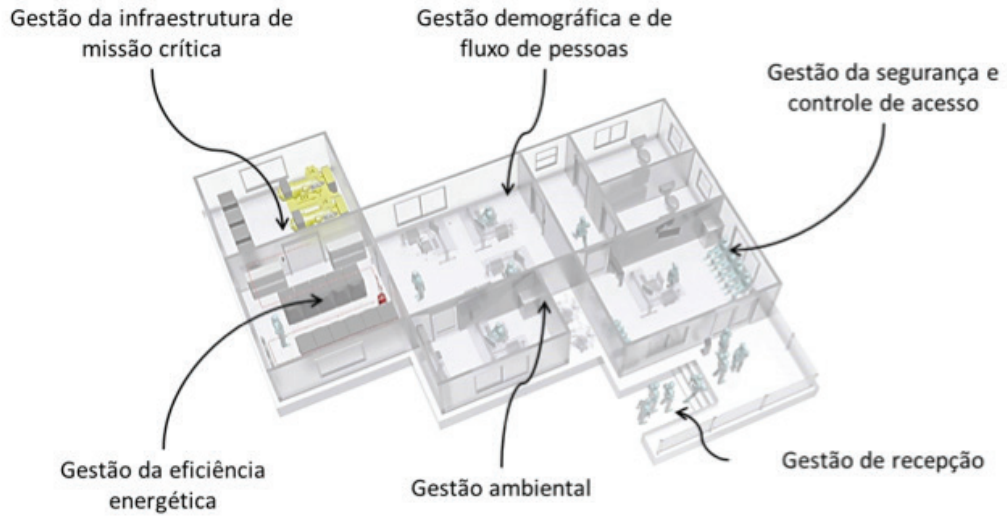
O estudo de caso descrito por Faccioni Filho (2015) se refere à nova geração de automação predial, em que o *design* é amparado pelo conceito da Internet das Coisas. O modelo do sistema parte de uma visão ampla do ambiente a monitorar e automatizar, e dispõe de todos os sistemas que deverão coexistir e cooperar na rede interna predial.

Veremos, na Figura 3.7, o ambiente típico para a solução de automação predial, baseada em conceitos de IoT. Mas antes de definir as "coisas" que farão parte de cada processo ou sensoriamento, há uma visão dos subsistemas de gestão, conforme as seguintes divisões:

- Gestão ambiental: refere-se aos sensores, automação e controle de temperatura, umidade, luminosidade, qualidade do ar, vazamentos de água, incidência solar, entre outros.
- Gestão da eficiência energética: refere-se aos sensores, automação e controle de uso de energia pelos mais diversos equipamentos presentes na edificação, bem como por outros sistemas que possam interferir no consumo de energia[8].
- Gestão de recepção: refere-se a sistemas para auxiliar na recepção, triagem e organização da entrada e saída de pessoas e produtos na edificação, otimizando a relação da edificação com os ambientes externos.
- Gestão de segurança e controle de acesso: refere-se aos sensores, automação e controle da segurança predial, tanto do ponto de vista patrimonial, como da segurança de vida, o que inclui sensores de fumaça, variação de calor, sensores de vibração, inundação e outras anomalias, bem como câmeras em circuito fechado de televisão, controle de acesso e intrusão.
- Gestão demográfica e de fluxo de pessoas: refere-se aos sensores, automação de controle do fluxo ótimo de pessoas na edificação, com dispositivos de presença e outros controles de acesso, operando em conjunto com a gestão de recepção e gestão de segurança, visando ao melhor aproveitamento dos espaços prediais.
- Gestão da infraestrutura de missão crítica: refere-se aos sensores, automação e controle dos ambientes críticos da edificação, como os de energia, água, comunicações e informática, que, por princípio, devem ser resilientes e com alta tolerância a riscos, permitindo operação contínua da edificação.

8. Como, por exemplo, fluxo de ventilação natural, incidência solar etc.

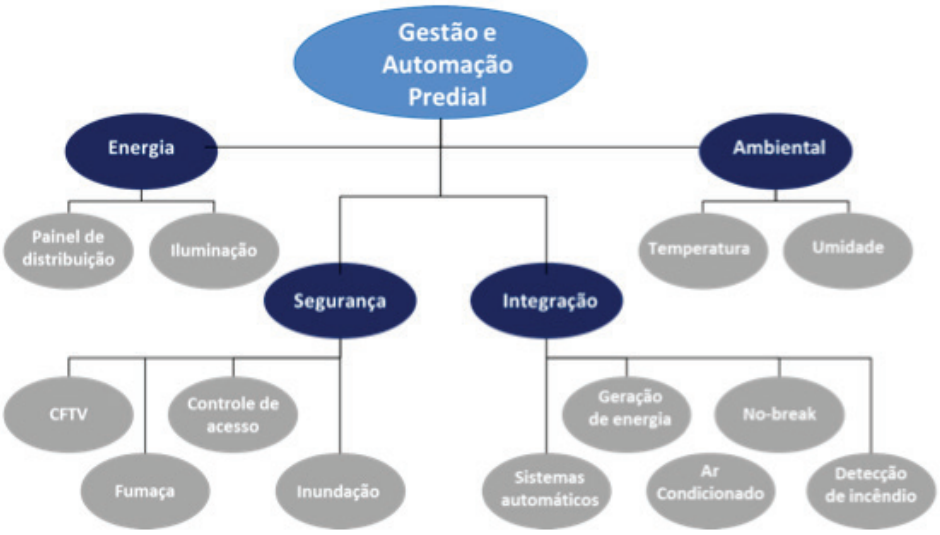
Figura 3.7 – Gestão e Automação Predial baseada em IoT



Fonte: Elaboração do autor, 2016.

A partir dessas considerações e da visão global e integrada da edificação, um novo modelo se impõe, partindo dessa visão tridimensional dos ambientes e seus sistemas gerais. O desenvolvimento da plataforma de automação, baseada em IoT, permite criar um diagrama que distribui as funcionalidades e suas particularidades, para, então, distribuir os objetos ("coisas") entre os diversos subsistemas. Esse diagrama está representado na Figura 3.8, onde cada objeto agrega funcionalidades de acordo com sua função no sistema, podendo servir a um ou mais subsistemas.

Figura 3.8 – Diagrama esquemático de plataforma de automação predial



Fonte: Elaboração do autor, 2016.

A gestão predial é um exemplo prático do uso da IoT no mercado atual:

- Pode configurar soluções simples, como a automação de temperatura e umidade numa rede local em que sensores e atuadores atuam conjuntamente para obter o melhor ambiente, a partir das premissas de configuração na rede; ou
- pode ser um sistema complexo e interligado de subsistemas de gestão, como o apresentado na Figura 3.8.

Inúmeras outras aplicações da IoT estão surgindo, e o futuro breve promete um conjunto interligado de soluções, tanto em ambientes e processamento locais (*Fog*), como em grandes sistemas multiuso (*Cloud*).

Referências

AEGIS. **M2M application characteristics and their implications for spectrum**: Final Report. Aegis Systems Limited, 2014. Disponível em: <http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf>. Acesso em: 26 ago. 2016.

ALLEN, Mary. Distributed intelligence and IoT fog. **InsightaaS**. 06 ago. 2014. Disponível em <http://insightaas.com/distributed-intelligence-and-iot-fog-2/>. Acesso em: 25 ago. 2016.

Banafa, Ahmad. Internet of Things (IoT): Security, Privacy and Safety. **New Trends in Hi Tech by Ahmed Banafa**: Internet of Things (IoT) , Big Data , Cloud Computing and Mobility. 09 mar. 2015. Disponível em: <http://ahmedbanafa.blogspot.com.br/2015/03/internet-of-things-iot-security-privacy.html>. Acesso em: 25 ago. 2016.

COMSOC. **Infographic**: Internet of Things (IoT). 2015. Disponível em: <http://www.comsoc.org/blog/infographic-internet-things-iot>. Acesso em: 26 ago. 2016.

FACCIONI FILHO, Mauro. BMS 2.0 - Nova geração de sistemas de automação e gestão predial. **Congresso Netcom**, São Paulo, Aranda Eventos, 2015.

GREENOUGH, John; CAMHI, Jonathan. Here are IoT trends that will change the way businesses, governments, and consumers interact with the world. **Business Insider**. 15 jul. 2016. Disponível em: <http://www.businessinsider.com/top-internet-of-things-trends-2016-1>. Acesso em: 26 ago. 2016.

RICHMOND, Shane. Wearable computing is here already: How hi-tech got under our skin. **Independent**. 19 jul. 2013. Disponível em: <http://www.independent.co.uk/life-style/gadgets-and-tech/features/wearable-computing-is-here-already-how-hi-tech-got-under-our-skin-8721263.html>. Acesso em: 26 ago. 2016.

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. **The Internet of Things**: An Overview. Geneva, Switzerland: The Internet Society (ISOC), 2015.

TRANS COMMUNICATIONS. **Telemetry**. [201?]. Disponível em: <http://www.transcommunications.com.au/telemetry>. Acesso em: 22 ago. 2016.

Considerações finais

Neste trabalho, vimos como a Internet das Coisas se desenvolveu a partir da confluência da internet com os sistemas RFID e outras redes sem fio de automação. Outras influências importantes são de cunho conceitual, mais do que tecnológico. Nesse foco, temos a formação de redes multiprotocolos, interação entre sistemas diversos e multidisciplinares, bem como ecossistemas que a Internet das Coisas é capaz de abarcar.

Um dos conceitos principais, e que merece destaque, é que a Internet das Coisas, ou IoT, não é uma tecnologia, mas um conjunto de tecnologias e topologias integradas, operando tanto em macroestruturas (digamos, “cloud”) como em microestruturas (digamos, “fog”). A própria arquitetura da IoT traz esse conceito, e cada último componente, ou “coisa”, comporta capacidade de processamento e comunicação, tornando-a “inteligente”. E, assim, a palavra “inteligente” vem acompanhando muitas plataformas de mercado, como o *smart grid, smart city, smart building* e muitos outros.

Por fim, a realidade da IoT já mostra sua face no mercado. Aparelhos e roupas de uso diário, os wearables, são uma realidade e empresas estão se dedicando a desenvolver novos produtos, sendo que várias dessas empresas já são milionárias. Nem precisamos citar o Google ou a Apple, que investem fortemente nesse setor, em itens aparentemente simples, como óculos e relógios, até vastas estruturas de geolocalização e rastreamento global. A IoT é um ambiente de desafios para todos nós: tanto para as grandes empresas, quanto para os desenvolvedores e designers individuais.

Está aberta a temporada de oportunidades, bom trabalho a todos!

Sobre o conteudista

Mauro Faccioni Filho

Graduado em Engenharia Elétrica pela Universidade Federal de Santa Catarina (UFSC), em 1985. Mestrado e doutorado em Engenharia Elétrica pela UFSC, em 1997 e em 2001, respectivamente. Durante a pesquisa do projeto de mestrado, em 1999, realizou estágio na University of Nottingham, Inglaterra. Pós-Doutorado no tema “Social Network Analysis” pela University of London, Queen Mary College, em 2006.

Na UFSC, foi colaborador em pesquisas de eletromagnetismo e modelagem numérica no Laboratório Maglab, de 2001 a 2003. Diretor do Centro de Tecnologia em Automação e Informática, CTAI/SENAI, de 2002 a 2004.

Em Literatura, publicou livros de poesia (Olhos cegos, Editora Letras Contemporâneas, 2004; Duplo dublê, Editora Letras Contemporâneas, 2002; Helenos, Editora Letras Contemporâneas, 1998. Coeditor da Revista Babel, Poesia e Crítica, de 2000 a 2002.

Certificado ATD pelo Uptime Institute (USA) e membro do comitê CE-03:046.05, Norma 14565:2013 da ABNT. Recebeu, em 2012, pelo desenvolvimento da plataforma de software *DataFaz DCIM*, o prêmio “Ideia para o Futuro & Conceitos de Design”, do DatacenterDynamics Awards.

Diretor e sócio-fundador das empresas Fazion Sistemas Ltda (plataformas e aplicativos para celulares) e Creare Fazion Ltda (soluções de infraestrutura e automação para Data Centers).

Coordenador e professor de curso superior e de pós-graduação da Universidade do Sul de Santa Catarina (UNISUL), na modalidade da educação a distância (UnisulVirtual).

UNISUL

www.unisul.br