UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Internet das Coisas e a integração de sistemas domóticos residenciais: o protocolo *KNX*

Pedro Luís Teixeira Pimparel

Dissertação para obtenção do Grau de Mestre em
Engenharia Eletrotécnica e de Computadores
2º ciclo de estudos

Orientador: Prof. Doutor António Eduardo Vitória do Espirito Santo
Covilhã, outubro de 2017

Dedicatória

Gostaria de dedicar este trabalho à minha família, esposa (Sónia Rosa Barata Aradas Pimparel) e filhos (André Pedro Aradas Pimparel e Beatriz Aradas Pimparel), elos importantes na minha vida que em tudo me apoiaram para que este trabalho fosse possível.

Agradecimentos

Não poderia chegar aos términos desta dissertação, sem antes, deixar bem expresso um enorme reconhecimento ao meu orientador, Professor António Espirito Santo pela disponibilidade e afabilidade manifestada na orientação deste trabalho bem como pelo excelente trabalho como Diretor de Curso.

Mas há também outras tantas pessoas a quem terei que estender este meu reconhecimento, pois a sua cooperação foi fulcral para a consecução desta tese. Assim, agradeço:

- à minha querida esposa, pelo cooperação manifestada, bem como pela paciência nos momentos de inquietação e cansaço partilhados em conjunto;

- aos meus estimados pais e sogros, pelo apoio incondicional em todos os momentos, pelo encorajamento manifestado na minha inscrição no mestrado;

- aos meus lindos filhos, André e Beatriz pela ternura e carinho que sempre me dedicaram;

- à restante família e amigos, que de variadas formas, contribuíram para o resultado desse trabalho.

Resumo

A Internet das Coisas e a integração de sistemas domóticos residenciais foi o tema desenvolvido, neste trabalho, como o propósito explorar este conceito, atualmente muito discutido no mundo académico e empresarial e fazer a sua ligação com a domótica residencial.

A sequencia dos capítulos apresentados, foi estruturada para fazer a ponte entre a Internet das coisas e a domótica residencial. O trabalho inicia com o enquadramento e objetivos. Seguidamente introduz o tema da Internet das Coisas como ponto de partida para o desenvolvimento do trabalho propriamente dito. Segue-se a apresentação do conceito de domótica assim como dos seus princípios e alguns dos protocolos mais utlizados a nível mundial. Dando seguimento a um dos objetivos propostos, o estudo de um protocolo de domótica, apresentam-se as vantagens do protocolo *KNX*, face a outros protocolos, e aprofunda-se o estudo do mesmo. Tendo em conta o tema explica-se em pormenor como se processa a transferência de informação, neste protocolo, em *IP* e as soluções atuais do mercado para a ligação dos dispositivos *KNX* com a Internet. Apresentam-se os dois tipos de dispositivos de ligação utilizados que são as *Gateway KNX IP* e as *Gateway Web Service KNX IP* assim como o seu principio de funcionamento. Por fim, apresenta-se a evolução que terão os dispositivos *KNX* ao longo dos próximos anos, para facilitar a ligação à Internet no âmbito da Internet das Coisas.

Paralelamente ao desenvolvimento teórico elaborou-se um trabalho prático com vista a validação experimental dos métodos atuais de ligação dos dispositivos domóticos *KNX* à Internet. Planificou-se e construi-se uma maqueta com um sistema domótico *KNX* e apetrechou-se com os componentes necessários para a ligação dos componentes instalados à internet. Foram validados dois métodos utilizando respetivamente os dois componentes diferentes, o Gatewat *KNX IP* e a *Gateway Web Service KNX IP*, que funcionaram em ambos os casos.

Por fim, neste documento, apresentaram-se as considerações finais sobre o trabalho desenvolvido, relevância para a minha atividade pessoal e profissional assim como a importância do mesmo para trabalhos futuros.

Palavras-chave

Internet das Coisas, *IoT*, domótica residencial, *SmartHome*, *KNX*, *Gateway*, *Router KNXnet/IP*, *Gateway WS KNX*, *KNX* sobre *IP*.

Abstract

The Internet of Things and the integration of home domotic systems was the theme developed in this work, with the purpose of exploring this concept, currently much discussed in the academic and business world, and making its connection with home automation.

The sequence of the chapters presented was structured to connect the Internet of things with home automation. This work begins with its framework and objectives. It then introduces the topic of the Internet of Things as a starting point for the development of the work itself. After that, we have the presentation of the concept of home automation as well as its principles and some of the protocols most used worldwide. Then, we have one of the proposed objectives : the study of a home automation protocol, presenting the advantages of the KNX protocol, compared to other protocols, and we deepen its study. Taking the topic into account, we explain in detail how to transfer information in this protocol, IP and the current market solutions, to connect KNX devices to the Internet. The two types of connection devices used are the KNX IP Gateway and the Gateway KNX Web Service IP, as well as their operating principle. Finally, the evolution of the KNX devices over the next few years is presented, in order to facilitate Internet connection in the Internet of Things.

In parallel with the theoretical development, a practical work was developed to validate the current methods of connecting KNX home automation devices to the Internet. A model was planned and constructed with a KNX home automation system and equipped with the necessary components for the connection of the installed components to the Internet. Two methods were validated using the two different components, Gatewat KNX IP and Gateway Web Service KNX IP respectively, which worked in both cases. Lastly, we present in this document the final considerations on the work developed, their relevance to my personal and professional activity, as well as their importance for future work.

Keywords

Internet of things, IoT, Home domotic systems, SmartHome, KNX, Gateway, Router KNXnet/IP, Gateway WS KNX, KNX on IP.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

AM	*Application Module*
ARP	*Address Resolution Protocol*
ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
BCU	*Bus Coupling Unit*
BIM	*Bus interface module*
Cisco (IBSG)	*Cisco Internet Business Solutions Group*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
DDNS	*Dynamic Domain Name System*
DEM	Departamento de Engenharia Eletromecânica
DIN	*Deutsches Institut für Normung*
DNS	*Domain Name System*
DoS	*Denial of Service*
EEPROM	*Electrically-Erasable Programmable Read-Only Memory*
EIB	*European Installation Bus*
ETS	*Engineering Tool Software*
FTP	*File Transfer Protocol*
HES	*European Home Systems Association*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
HVAC	*Heating, Ventilation and Air Conditioning*
ICMP	*Internet Control Message Protocol*
IEEE	*Institute of Electrical and Electronic Engineers*
IGMP	*Internet Group Management Protocol*
IoT	*Internet of Things*
IP	*Internet Protocol*
IV	Infravermelho
KNX WS	*Web Services KNX*
LAN	*Local Area Network*
MILNET	*Military Network*
MIT	*Massachusetts Institute of Technology*
OBIX	*Open Building Information Exchange*
PEI	*Phisical External Interface*
PL	*Power Line*
RAM	*Random Access Memory*
RF	Rádio frequência
ROM	*read-only memory*
SFSK	*Spread frequency Shift Keying*
SMTP	*Simple Mail Transfer Protocol*
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transfer Protocol*
TI	Tecnologia da informação
UBI	Universidade da Beira Interior
UDP	*User Datagram Protocol*

USB	*Universal Serial Bus*
VPN	*Virtual private network*
WAN	*wide area network*
WS	*Web Services*
XML	*Extensible Markup Language*

Capítulo 1 – Introdução

1.1. Enquadramento

Com a *Internet* das Coisas (*IoT* do inglês *Internet of Things*), surge um novo paradigma onde é possível a conexão entre dispositivos a partir de aplicações desenvolvidas sem, necessariamente, envolver uma interface homem-máquina. É considerada uma revolução semelhante à revolução industrial do Séc. XIX. A diferença substancial neste novo conceito está na forma de conexão entre dispositivos, uma vez que será possível a sua interligação, sem intervenção humana [1].

A ideia de ligar dispositivos começou a seu discutida a partir dos anos 1991, 1992 quando a conexão *TCP/IP* e a *Internet*, como é conhecida hoje, começou a difundir-se [2]. O termo "*Internet* das Coisas" foi proposto em 1999, por *Kevin Ashton* do *MIT*, juntamento com a sua equipa tendo escrito, este investigador, um artigo dez anos depois, para o *RFID Journal*, denominado "A Coisa da *Internet* das Coisas". Segundo este, a "*Internet* das Coisas", é uma revolução tecnológica cujo o objetivo principal é a conexão entre todos os equipamentos utilizados no dia-a-dia e a *Internet* [3], a *IoT*. Estudos, levados a cabo pela Cisco (2013), indicam que 99,4% dos objetos físicos estariam desconectados das redes, mas com os avanços tecnológicos, tenderiam a estar aptos a fazer parte da "*Internet* das Coisas" tornando a sua conexão efetiva [4]. Estão à disposição, sensores, atuadores e dispositivos praticamente impercetíveis, prontos a serem introduzidos no nosso dia-a-dia, que podem ser ligados à *Internet*, sem que notemos e sem que alterem as nossas rotinas, o que faz com que o número de dispositivos ligados esteja constantemente a aumentar. De acordo com o Cisco IBSG, a *IoT* começou no momento em que foram ligados, à *Internet*, mais dispositivos do que pessoas. Nestes dispositivos incluímos smartphones, eletrodomésticos, computadores, e sensores inteligentes, entre outros, que estejam ligados à *Internet*. Podemos enquadrar a data de ocorrência deste evento entre 2008 e 2009, Figura 1 [5].

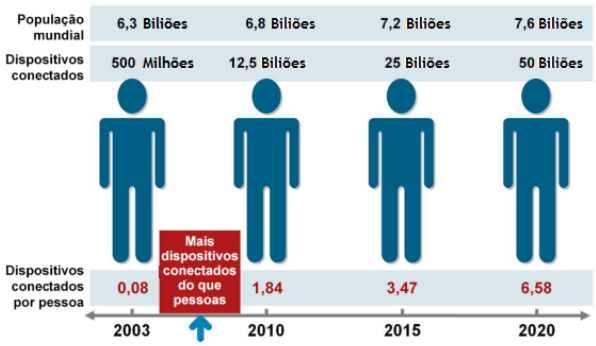


Figura 1: Previsão da evolução do número de dispositivos conectados à *Internet* até 2020.

A conexão entre diferentes dispositivos e a *Internet*, a *IoT*, assume atualmente uma relevância de tal ordem que a maior parte das grandes empresas de TI, Tecnologias de informação (de *IT*, *Information Technology*) procuram soluções nesta área. A empresa CISCO estima que 14,4 triliões de dólares é o valor em jogo para as companhias e indústrias nesta fase inicial, mas, até 2022, este valor deverá aumentar significativamente [6]. O interesse varia em áreas como a indústria, defesa, saúde, comércio, entre outras. A área residencial também não é exceção. É justamente nesta área que incide este trabalho. Esta é uma área com forte crescimento, nomeadamente na área da automação residencial associado ao conceito de *SmartHome*, com a utilização da Domótica. A palavra Domótica deriva da palavra "*Domus*" que significa Casa e da palavra "Telemática" que deriva das palavras Telecomunicações e Informática (Dom+ó+tica = Domótica) [7]. Hoje em dia é possível a interligação, com a domótica, das várias partes de uma habitação, nomeadamente iluminação, aquecimento, controlo de acessos, e outras. Numa *SmartHome* utiliza-se a domótica para reduzir a utilização de tarefas rotineiras, mas essenciais como por exemplo o controlo automático da temperatura de uma habitação, a rega automatizada, ou a adequação da iluminação à luz ambiente.

1.2. Motivação

Nas várias áreas de atuação da domótica, a domótica residencial é aquela com mais forte crescimento, prova disto mesmo é o lançamento de produtos, nesta área, pelos gigantes mundiais da industria, de salientar apenas o caso da *Google* com o *Google Home*, a *Apple* com *HomeKit* e para finalizar o exemplo a *Amazon* com o seu *Amazon Echo*. Embora estes produtos dispensem instalador e conhecimentos avançados na área das TI apresentam atualmente recursos limitados. Curiosamente aplicações destas mesmas empresas podem gradualmente ser introduzidas nas instalações de domótica convencionais podendo ser uma mais valia para as mesmas, pois por exemplo a *Google Home* pode utilizar comandos de voz para introduzir alterações nos componentes da instalação. Atualmente muitas das tarefas de uma casa podem ser executadas de forma automática, pode-se fazer a monitorização e visualização do estado dos vários componentes, a partir de um *tablet*, *smartphone* ou qualquer outro dispositivo móvel, seja localmente ou remotamente. Em Portugal, esta é uma área com pouca implementação prática, comparada com outros países da europa, existindo um forte potencial de crescimento. A Figura 2 [8], mostra uma comparação do investimento realizado, em domótica residencial, em alguns países da europa. Em 2015 o valor gasto estimado, nos países representados, nesta área, foi de 371 milhões de euros. Estes valores evidenciam a importância do sector na economia. Salientar apenas que, por habitante, a Noruega é o país que mais gasta, uma média de 3,5 €/por ano. A Suíça ocupa o 2º lugar seguida da Alemanha.

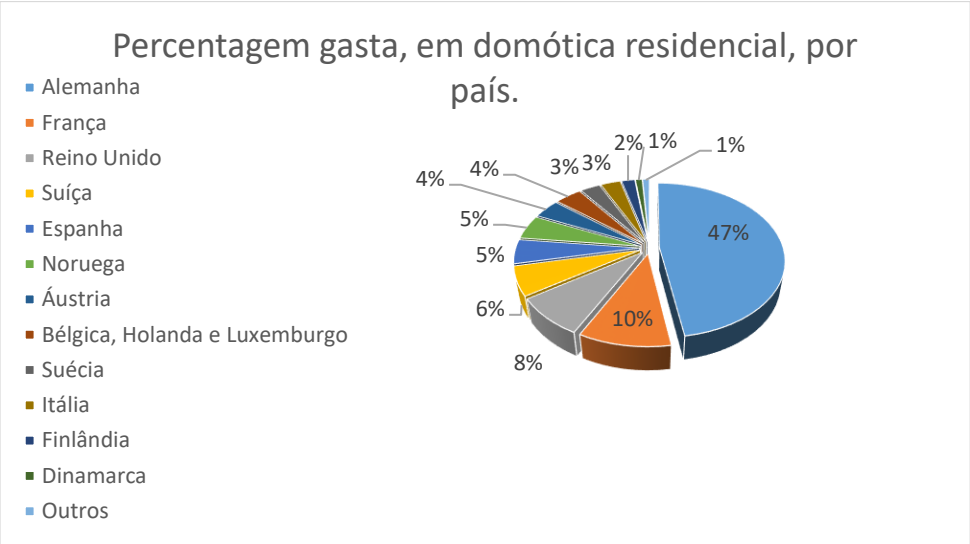


Figura 2: Percentagem do valor gasto por ano em 2015, em domótica residencial em alguns países da Europa.

A Figura 3 [8], mostra a distribuição do investimento, na domótica residencial, por áreas como a segurança, conforto/economia de tempo, eficiência energética e motorizações. Verifica-se que é na segurança (incluindo a vídeo vigilância) que está a maior fatia do investimento.

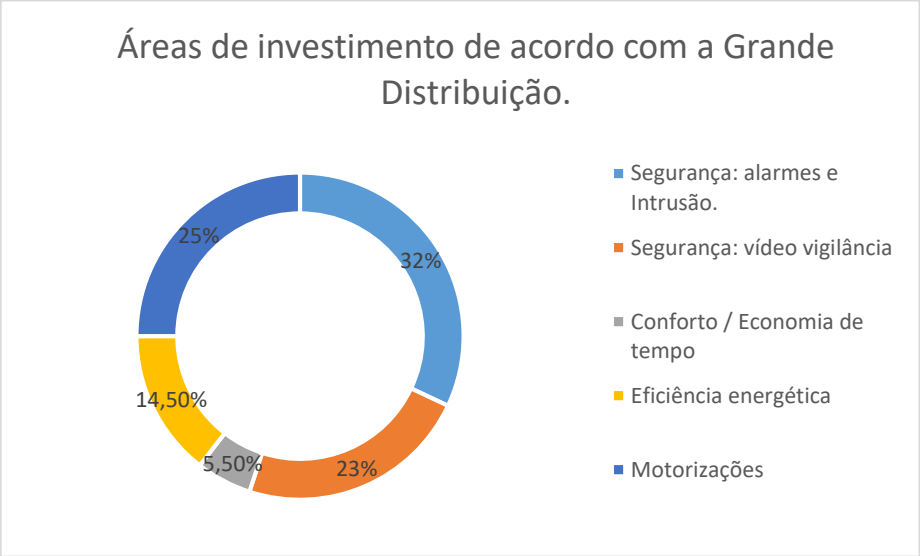


Figura 3: Áreas de investimento em domótica residencial.

Incrementando ao conceito de domótica residencial o conceito de *IoT* surge uma área onde a inovação estará presente, com a necessidade de introdução de novos produtos uma vez que surgem infinitas novas possibilidades. Percebe-se que esta área terá um forte crescimento durante os próximos anos. As diferentes áreas, que domótica residencial abrange, permitirá que facilmente se transporte para outros segmentos de mercado, por exemplo escolas, escritórios, hotéis, entre outros. A nível pessoal e profissional sempre vi o trabalho final como uma necessidade de incremento do conhecimento teórico e prático e esta área será certamente uma mais-valia no curto e longo prazo.

1.3. Objetivos

Neste trabalho pretende-se explorar o conceito de domótica, em particular o de domótica residencial e conhecer principais aspetos técnicos a ter em conta nesta área. Conhecer em pormenor um protocolo de domótica, preferencialmente abrangente, nas diferentes áreas de investimento residencial como conforto, segurança e, eficiência energética. Conhecer as soluções de integração da domótica, na Internet. Pretende-se ainda explorar a noção de *IoT* na área da domótica residencial e respetiva análise de potencialidades. Pretende-se desenvolver um trabalho prático de validação experimental com soluções para a integração da domótica residencial na *IoT*.

1.4. Organização da Tese

Este trabalho está estruturado em capítulos. No primeiro capítulo resume-se a História da *Internet*, o aparecimento do protocolo *IP*v6 associado ao conceito da *IoT*. De seguida desenvolve-se o conceito de domótica residencial com apresentação das caraterísticas do protocolo *KNX*. Posteriormente, faz-se a ligação deste protocolo à *IoT*. Finaliza-se com a apresentação de soluções práticas que permitem o acesso de um sistema domótico, em maquete, à Internet. Por fim apresentam-se cenários presentes e futuristas relacionados com o conceito de domótica residencial e a noção de *SmartHome*.

Capítulo 2 – Breve história da evolução da *Internet*. A *IoT*

2.1. Breve história da *Internet*

A *Internet* está num caminho firme de desenvolvimento e aperfeiçoamento, no entanto não mudou muito desde o seu início. Ela faz essencialmente o mesmo de quando foi projetada, na era da *ARPANET*, 1969. A *Advanced Research Projects Agency Network (ARPANET)*, nos USA, foi responsável pela criação da primeira rede de computadores, para troca de pacotes de dados, entre as mesmas. Esta agência efetuava a sua pesquisa para fins militares. No final da década de 70, com um número crescente de utilizadores, divide-se e origina a *MILNET* que continua para o mesmo fim, o militar, e surge uma parte pública, cujo o nome é *Internet*. Esta ultima, atualmente, serve utilizadores de todo o mundo e passou a ser um sistema global de interligação de redes de computadores. Foram vários os protocolos de comunicação utilizados, mas o atual e protocolo padrão é o *IP* [5]. Este protocolo permite endereçar, isto é, atribuir uma identificação inequívoca a cada dispositivo conectado, na rede, de modo a que cada um seja identificado.

A transmissão de dados na rede é possível, fisicamente, graças a um conjunto de dispositivos que permitem que os dados circulem e sejam transmitidos/ transferidos. Como qualquer outro idioma, o idioma de *networking* utiliza um conjunto comum de símbolos para representar os dispositivos finais de uma rede. O reconhecimento destes componentes físicos de *networking* e as suas representações lógicas é fundamental para a visualização e organização operacional de uma rede. A Cisco, por exemplo, utiliza as representações da Figura 4 que serão adotadas, neste trabalho.

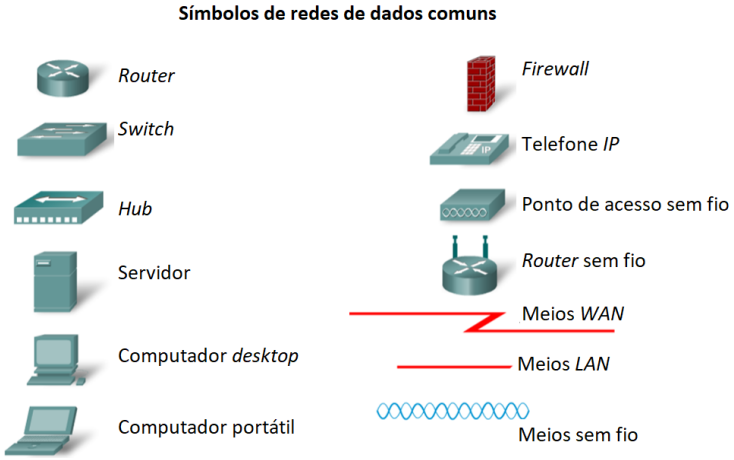


Figura 4: Representações lógicas dos componentes físicos de *networking* de uma rede.

Associada à *Internet* surgiram e evoluíram um conjunto de serviços e recursos de informação. Destaca-se a *Web* que teve várias fases de desenvolvimento. Inicialmente, a *Web* era utilizada, principalmente, no meio académico sobretudo para pesquisas. A segunda fase da *Web*, que pode ser chamada de "*panfletoware*" ficou caracterizada pela corrida aos nomes de domínio. Também conhecida como *Web* 1.0, esta etapa caraterizou-se pela necessidade de quase todas as empresas compartilharem informações na *Internet* para que as pessoas pudessem conhecer os seus produtos e serviços. A terceira fase da evolução, surgiu a partir de um patamar onde os dados estáticos passaram para informações transacionáveis, nas quais produtos e serviços passaram a ser comprados e vendidos. Foi nesta fase que surgiu a oferta de serviços e empresas *dotcom* como o *eBay* e a *Amazon* demarcaram-se claramente. Esta fase ficou conhecida como a do crescimento e explosão do "ponto com". Na quarta fase, fase atual, conhecida pela "*Web* Social" ou de "experiência", as empresas como *Facebook, Twitter* entre outras tornaram-se mundialmente conhecidas e, acima de tudo, muito rentáveis. Caraterística diferente da fase anterior. Atualmente, as pessoas podem comunicar, conectar-se e compartilhem informações (textos, fotos e vídeos) sobre si, com amigos, família e colegas [5]. Mas, paralelamente à *Web*, existem muitos outros serviços que utilizam protocolos próprios, por exemplo, o email. Na Figura 5 [9] estão sintetizados alguns dos protocolos atuais que permitem a ligação dos utilizadores através da Internet.

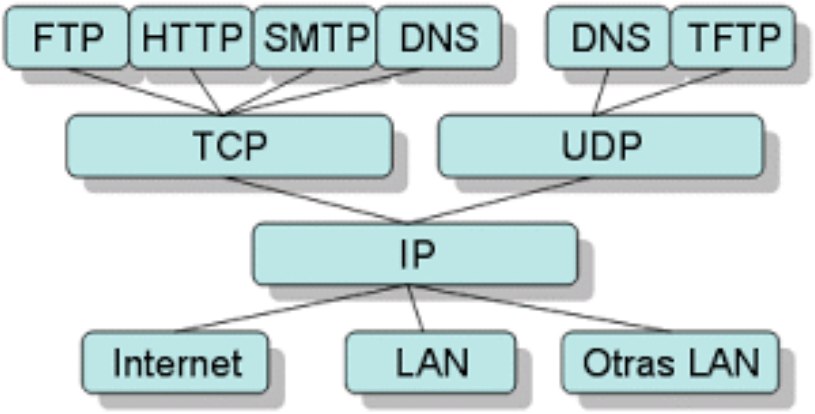


Figura 5: Alguns dos protocolos que permitem a ligação, dos utilizadores, através da Internet.

Chegamos à *Internet* das Coisas (do inglês *Internet of Things (IoT)* Figura 6 *)* que, em poucas palavras, não é mais do que uma extensão da *Internet* atual. Esta extensão é feita ao proporcionar que objetos do dia-a-dia (quaisquer que sejam) se conectem à *Internet* [10]. A principal diferença deve-se ao facto de estes dispositivos, ou objetos, poderem comunicar e trocar informação entre si, permitindo uma ligação entre o mundo real e o mundo da computação através da Internet [5]. Na Figura 6 [11] pretende-se transmitir esta ideia de que tudo está ligado entre si, isto é a *IoT*.

Figura 6: "Ideia" de ligação entre tudo, isto é a *IoT*.

2.2. Evolução do padrão *IP*V4 para *IP*V6

Os Protocolos associados *IP* (*Internet Protocol*) e *TCP* (*Transmission Control Protocol*) são os principais dentro de um conjunto de protocolos que direcionam o trafego e o funcionamento da *Internet*. O protocolo *IP* é o responsável por endereçar e encaminhar os pacotes de dados na *Internet*. Associado ao crescimento do número de dispositivos conectados à *Internet*, surgiu a necessidade de migração do protocolo *IP*v4 para sua versão 6, conhecido como *IP*v6. A justificação está na limitação deste protocolo em vários níveis, principalmente ao nível da segurança e no número de dispositivos que permite endereçar para que se possam ligar entre si. Foi o aumento significativo do número de dispositivos ligados, incluindo os dispositivos móveis como *smartphones* e *tablets* que fez com que o endereçamento esgotasse.

2.2.1. O padrão *IP*v4

A versão mais utilizada do protocolo *IP* é a versão 4, que permite 32 *bits* de endereçamento. Na prática, permite, a atribuição de aproximadamente quatro biliões de endereços, que ficam disponíveis para que outros tantos dispositivos estejam diretamente conectados à *Internet*. Devido a constrangimentos do protocolo quer ao nível de segurança, mas acima de tudo devido ao seu estrangulamento, pois estes endereços *IP* esgotaram-se, uma vez que é elevado o número de dispositivos que estão conectados, como computadores, relógios e eletrodomésticos [3]. Este endereçamento esgotou-se em fevereiro de 2010 [5] e obrigou à migração do protocolo *IP* para a sua versão 6, conhecido como *IP*v6 [3].

2.2.2. O Padrão *IP*v6

A solução para o contínuo crescimento da rede foi a introdução gradual do protocolo *IP* na sua versão 6. Na prática não se verifica nenhum impacto nesta transição, uma vez que já se previa o estrangulamento da versão anterior e estudavam-se alternativas há alguns anos [3]. O *IP*v6 possui 128 bits, no seu campo de endereçamento, o que acarreta $3{,}4\times10^{38}$ endereços *IP*, ou seja, possibilita endereçar até 340.282.366.920.938.463.463.374.607.431.768.211.456

endereços únicos, considerado pelos especialistas suficientes para superar as necessidades durante as próximas décadas.

Este protocolo permitirá um crescimento, sem constrangimentos, da *IoT*, uma vez que potenciais biliões de novos de dispositivos surgirão e exigirão endereços *IP* os quais encontram-se disponíveis. Além disto, o *IP*v6 facilita a gestão de redes devido a recursos de autoconfiguração e oferece recursos de segurança melhorados [5]. Com o *IP*v6, o endereço *IP* de cada dispositivo será único, o que facilitará a mobilidade na rede se o mesmo for necessário, como é o caso de dispositivos móveis [3].

2.3. A *IoT* a primeira evolução da *Internet*

A *Internet* das Coisas emergiu dos avanços em várias áreas científicas como sistemas embutidos, microeletrónica, telecomunicações, e tecnologias de informações. É um tema atual quer a nível académico, quer ao nível da industria, acida de tudo porque se espera que venha a ter um impacto significativo em muitas áreas do quotidiano [10]. Os investigadores acreditam que esta nova realidade levará a novas aplicações que permitirão mudar e melhorar a forma de como as pessoas vivem, aprendem e trabalham. A *IoT* está a transformar a Internet em algo mais sensorial, uma vez que passa a ser possível termos acesso, em tempo real, a um conjunte de dados medidos como temperatura, pressão, luminosidade, humidade e muito mais, permitindo que sejamos mais proativos e menos reativos. A *IoT* veio para ficar, pois trata-se de uma inovação e como é sabido, a inovação é essencial para o progresso humano. Basta pensarmos que a *IoT* está a expandir-se para cenários novos, impensáveis até aqui. Por exemplo, já há pacientes que utilizam dispositivos ligados à Internet, nos seus corpos, para ajudar os médicos a efetuarem diagnósticos e determinar as causas de determinadas doenças. Sensores muito pequenos podem ser colocados em praticamente qualquer parte do planeta para efetuarem medições, por exemplo, em animais, postes elétricos, entre muitos outros e serem ligados à Internet. Existem já projetos que querem levar a Internet para o espaço, o programa IRIS (*Internet Routing in Space*) da Cisco é um exemplo disto mesmo. Por estes motivos a *IoT* é considerada a primeira evolução real da Internet.

2.3.1.A *IoT* hoje

Atualmente, a *IoT* é composta por várias redes diferentes, cada uma, com finalidades específicas. Em termos residenciais podemos encontrar várias redes, de salientar, a rede telefónica para comunicações, TV, *Dali* para a iluminação, *HVAC* utilizada no controlo do aquecimento / ar condicionado, entre outras. Mesmo ligadas entre si têm ficado confinadas a redes fechadas. Com a evolução da *IoT*, estas tenderão a estar ligadas a muitas outras redes levando gradualmente a aumento da segurança, análise e melhor gestão de recursos. Facilmente compreende-se que, esta nova realidade, trará um novo potencial e recursos cada

vez mais poderosos [5]. A Figura 7, exemplifica a *IoT* atualmente e algumas das necessidades imediatas (3) desta nova realidade.

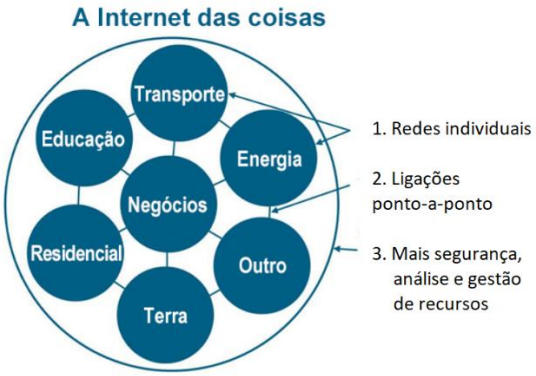


Figura 7: Modelo teórico da *IoT* hoje em dia com a ligação entre as várias redes.

Ao nível das ligações surgem problemas e novos desafios. Por exemplo, em 2014 a *Associação KNX* que representa um dos grandes padrões de domótica, a nível mundial, decidiu que seriam necessárias novas normas para facilitarem o alargamento da sua infraestrutura à *IoT*. Com o aparecimento inicial da Internet ocorreu uma situação idêntica, houve a necessidade de criar um padrão para unificar a rede, e o problema acabou por se resolver. Atualmente, a *IEEE* é apenas uma das organizações que trabalham para resolver estes desafios cujo o objetivo é o da troca de dados em *IP*v6 entre as várias redes. A resolução de problemas de incompatibilidade, nesta nova escala da *IoT*, ir-se-á resolver com o tempo. Outro problema que se coloca é o da autossustentabilidade de todos estes novos equipamentos, pois será impensável a troca constante de baterias em tantos equipamentos. Também na área do *Low Power* será necessária muito investigação, mas já há muitos progressos [5]. Salienta-se apenas a descoberta de novos constituintes para as baterias que as tornarão mais estáveis, duradouras e mais rápidas a carregar para além de se tornarem cada vez mais leves. Por outro lado, os novos sensores inteligentes capazes de recolherem a energia que precisam do ambiente que os rodeia [5].

2.3.2. A *IoT*: a noção de *Gateway*

As diferentes redes conectadas entre si, atualmente, como as que foram referidas anteriormente ou outras, para comunicarem precisam de um dispositivo chamado de *Gateway*. Pode ser utilizado com dois propósitos. O primeiro para o encaminhamento de mensagens entre as diferentes redes. Neste caso, o *Gateway*, funciona como intermediário entre tecnologias distintas para o encaminhamento de mensagens. Em segundo, o *Gateway* também pode ser um prestador de serviços da rede. Por exemplo, existem alguns que funcionam como um *proxy* que atuará como um intermediário, mas de serviços, entre os pedidos de recursos de outros servidores, efetuados pelos clientes [10]. Na Figura 8, mostra-se a configuração em duas situações diferentes para um *Gateway* utilizando o modelo de camadas, neste caso *UDP/IP*

(User Datagram Protocol) para troca de dados, em síntese, Aplicação, Transporte, Internet e Acesso à rede. O *Gateway*, ao centro, funciona como intermediário para o encaminhamento de dados (em cima) ou de troca de serviços (em baixo).

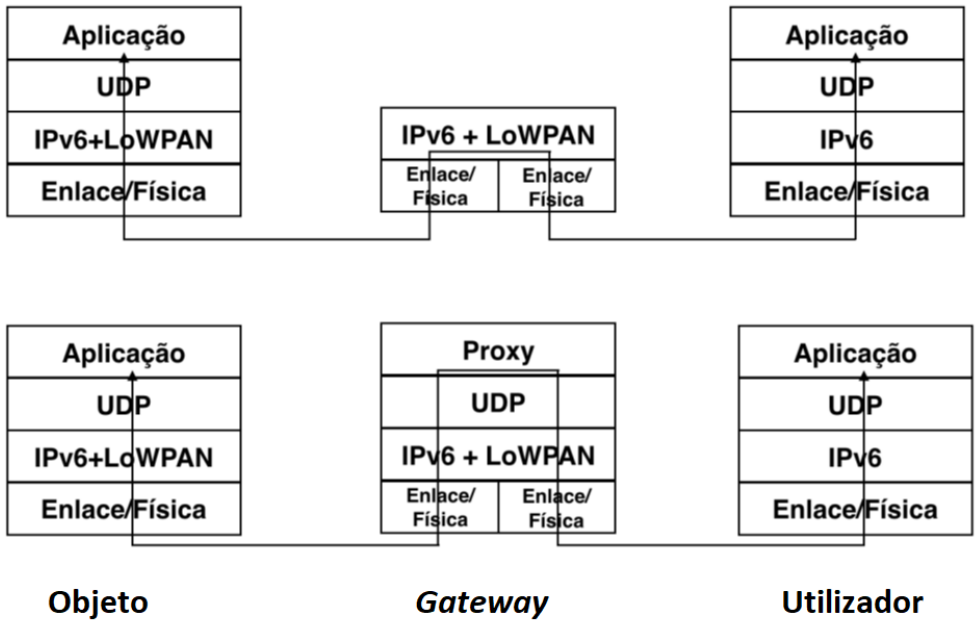


Figura 8: O *Gateway* como intermediário entre dois meios.

Por fim um, aspeto não menos importante é o da segurança. Para que um sistema *IoT* seja seguro é preciso traçar os objetivos de segurança adequadamente. Existem pelo menos três grupos de objetivos necessários para que *IoT* funcione adequadamente. Em primeiro, o da confidencialidade em que se exige que não se conheça o conteúdo numa comunicação na rede por terceiros. O segundo, o da integridade, isto é, em *IoT* deve-se assegurar que a informação chega de forma integral, sem que a informação seja alterada ou modificada. E, por fim, o da disponibilidade em que a rede deve estar sempre disponível e preparada contra o ataque de "hackers", por exemplo, do tipo *Denial of Service (DoS*). O suporte à segurança pode ser implementado nas diferentes camadas da pilha de protocolos, por exemplo, com a criptografia de dados.

Capítulo 3 - Domótica residencial. *SmartHome*. Análise comparativa

3.1. O conceito de Domótica. A domótica Residencial. Aplicações práticas

A domótica é cada vez mais utilizada e tem vindo a expandir-se ao longo dos últimos anos devido aos benefícios que a tecnologia associada a este conceito trás para os seus utilizadores. A domótica permite e facilita: uma gestão eficiente das instalações e dos equipamentos; a regulação automática térmica, ambiente; informação do estado das instalações, através de comunicação em tempo real, com a possibilidade de diagnósticos remotos; uma melhor eficiência energética; incremento de segurança às habitações; controlo de iluminação com cenários de ajuste automático em função da intensidade luminosa ambiente; gestão centralizada ou descentralizada das instalações. A automação residencial permite integrar e interligar a iluminação, o entretenimento, a segurança, as telecomunicações, o aquecimento, o ar condicionado através de um sistema inteligente programável que pode ser centralizado, ou não. Em qualquer edifício, os sistemas técnicos têm que cumprir os mesmos objetivos. Por exemplo: controlo de iluminação, persianas e toldes, controlo de aquecimento/ ar condicionado e ventilação individual de cada divisão, gestão de cargas elétricas, vigilância do edifício, controlo de acessos e comunicação com outros sistemas. A Figura 9 [12] mostra um exemplo de um sistema domótico.

Figura 9: Um sistema domótico permite interligar diferentes áreas de um edifício e facilitar o dia-a-dia dos seus utilizadores.

Convém esclarecer o conceito de *SmartHome* ou "Residência Inteligente", que é um conceito que está associado à Automação Residencial ou Domótica. Esta expressão, muito utilizada a nível de *marketing*, pode ser vista como os serviços prestados pelos diferentes equipamentos interligados num sistema domótico, em casa. Estas interligações conferem a estes edifícios caraterísticas especiais nas áreas do conforto, comunicações, energia e segurança. Um sistema domótico, com serviços adequados, aporta um conjunto de vantagens, a nível de economia de tempo, do conforto, da segurança do edifício, da poupança energética, da segurança de pessoas e bens, no entretenimento. Em síntese, facilita o dia-a-dia dos seus utilizadores. Na Tabela 1, são apresentados alguns serviços possíveis da domótica/ um sistema domótico, no dia-a-dia.

Tabela 1: Exemplos de aplicações de domótica.

Vantagens	Exemplos de aplicações com domótica
Eficiência energética	Programar de equipamentos de aquecimento ou arrefecimento para os horários adequados; Desconexão de aparelhos que não estejam a ser utilizados; Controle da iluminação em função da luz ambiente.
Segurança nos edifícios	Deteção de fugas de gás, inundações, incêndios com corte automático e alarmes; Avisos de janelas abertas em caso de esquecimento; Fecho de toldes ou portadas com ventos fortes.
Segurança de pessoas e bens.	Alarme de intrusão com aviso, em tempo real; Verificação de um perímetro de segurança; Monitorização de imagens com ligação à Internet para uma observação local e remota.
Conforto / Economia de tempo.	Ajustes automáticos das temperaturas de piscinas e aquecimento central com interface inteligente de acesso remoto; Informações diversas sobre humidade, temperatura, velocidade do vento; Sistemas de som centralizado; Estado *(On/Off)* dos equipamentos a partir de um dispositivo móvel; Controle dos mesmos a partir do telemóvel, tablet ou Computador; Criação de cenários, por exemplo ambientes diferentes em ocasiões diferentes; Rega automática.
Comunicação	Sistemas que funcionem com sensores ou voz e que facilitem o acesso aos equipamentos, inclusive a pessoas com necessidades especiais; Visualização remota de imagens.

3.2. Aspetos técnicos em domótica

Na domótica existem vários aspetos técnicos que devem ser considerados, salientam-se três que são o tipo de arquitetura implementada, isto é, o modo como os diferentes constituintes de uma instalação domótica se interligam, os meios de comunicação, que podem ser vários, mas fundamentais para a transmissão dos dados e, por fim, o protocolo de comunicação que permite que os diversos constituintes de um sistema domótico, por exemplo os sensores e atuadores, comuniquem entre si.

3.2.1. Arquitetura

Relativamente aos tipos de arquitetura, existem três que são fundamentais: a arquitetura centralizada, a arquitetura descentralizada e a arquitetura distribuída. A arquitetura centralizada, tem uma unidade de controle que é fundamental para a interligação dos vários sensores (S) e atuadores (A) na instalação. Este tipo de arquitetura é normalmente mais económico, mas se este componente falhar todo sistema deixa de funcionar. Na Figura 10 [13] podemos ver um exemplo de uma arquitetura centralizada [13].

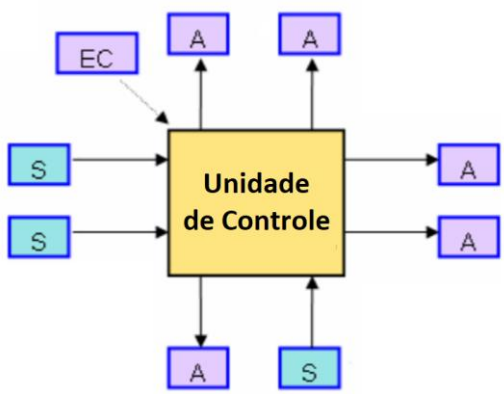


Figura 10: Arquitetura centralizada.

Nalguns casos podem existir mais do que uma unidade de controle, Figura 11. Este sistema é conhecido pelo sistema descentralizado. Em caso de falhas no sistema, os efeitos serão menos significativos do que no caso anterior.

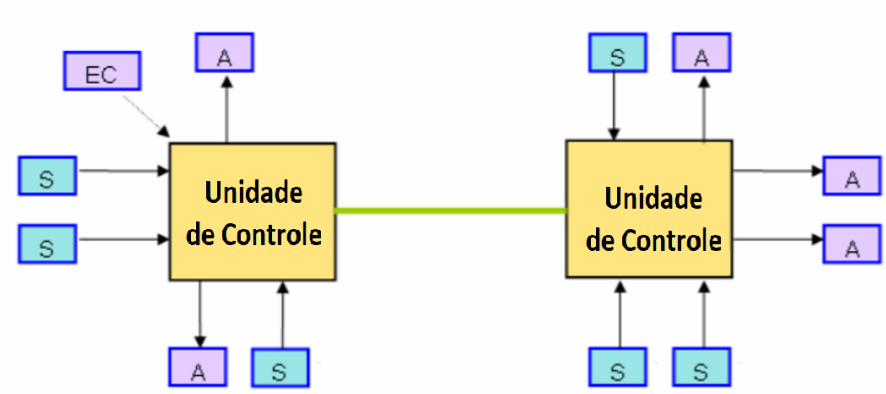


Figura 11: Arquitetura descentralizada.

Por fim, o sistema distribuído onde não é necessária nenhuma unidade de central controle. Neste caso, existe uma maior imunidade a falhas. Em caso de avaria, apenas é afetada uma

parte do sistema. Algo semelhante a uma instalação tradicional. Neste caso os componentes estão ligados entre si através do barramento.

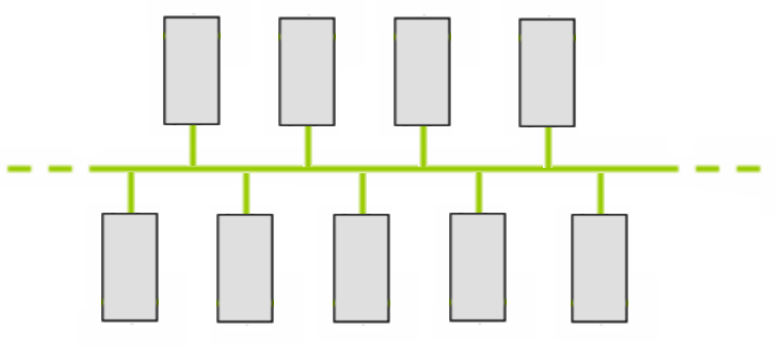


Figura 12: Arquitetura distribuída.

3.2.2. Meios de Comunicação

A comunicação é fundamental na domótica, uma vez que os dispositivos comunicam entre si uni ou bidireccionalmente. Torna-se essencial a existência de um meio de comunicação. Os meios de comunicação utilizados são a rede elétrica, o cabo coaxial, o cabo de baixa tensão (pares entrelaçados TP), radiofrequência (RF), Wi-Fi e infravermelhos (IV). O sistema que usa a rede elétrica para comunicar, permite aproveitar a instalação já existente e, por conseguinte, é o que acarreta menos despesas em obras para se obter uma instalação cablada. Pode obviamente ser utilizado em edifícios já construídas. Neste tipo de comunicação o que se faz é a injeção de um sinal de alta frequência, na linha de potência elétrica. Este tipo de infraestrutura fica sujeito ao ruído da rede sendo necessário que, os equipamentos de comunicação, tenham filtros adequados. A velocidade de comunicação tem vindo a aumentar significativamente, mas os padrões de comunicação já normalizados não permitem grandes velocidades. O padrão *KNX* ou o X-10 que permitem este tipo de meio não lidam com sinais digitais de alta resolução, por exemplo, para vídeo. Para contornar o problema, existem outros tipos de cabos como o cabo coaxial. É tipicamente um condutor isolado com uma malha protetora. Permitem transferir dados em alta frequência e a longas distâncias. A sua malha, que é ligada à terra, atua como um filtro às radiações externas que poderiam interagir com o condutor interno (indução eletromagnética) que é quem transporta a informação a alta velocidade. São utilizados para a transmissão de dados de vídeo e voz, mas as especificações técnicas destes cabos não lhe permitem transferir potência elétrica. Na domótica são ainda utilizados outros cabos de rede com pares trançados (*UTP)* que se dividem em várias categorias de acordo com caraterísticas técnicas. É uma cablagem de baixa tensão que pode operar entre os 5 V e os 30 V. Estes cabos são entrelaçados para que seja anulado o efeito dos campos magnéticos mútuos por eles criados. Outro meio é a radiofrequência, através de ondas eletromagnéticas, que tem grandes potencialidades na automação residencial pois pode

permitir a ligação sem fios e não requer alteração de instalações já existentes. Dado que as ondas de RF atravessam obstáculos, não é necessário colocar os emissores visíveis aos recetores. Em termos de desvantagens temos a vulnerabilidade a ruídos e interferências e pode ocorrer em função da potência dos aparelhos que o alcance não seja o ideal, podendo levar a falhas em determinadas zonas do edifício. Por outro lado, se não houver encriptação de dados pode haver problemas de segurança nas transmissões. Mais recentemente temos equipamentos ligados por Wi-Fi, ao encontro da *IoT*. Como os sinais, se transmitem por ondas eletromagnéticas levantam os mesmos problemas da RF. Os infravermelhos são utilizados para comunicação unidirecional normalmente com aparelhos já existentes como por exemplo Televisões, ar condicionado, entre outros [12] [14].

3.2.3. Elementos de um sistema domótico

Os sistemas domóticos são constituídos pelos seguintes elementos: sensores, atuadores, controladores, as interfaces e dispositivos específicos. Os sensores convertem em informação analógica ou digital informações do meio, como por exemplo, o toque num interruptor, o movimento de pessoas, ou a temperatura de uma habitação. Por outro lado, os atuadores realizam as instruções necessárias de elementos como electroválvulas, motores, entre outros. Os controladores, gerem a instalação, ou parte dela. As interfaces efetuam a ponte entre a infraestrutura domótica e os utilizadores permitindo a troca de informação. Podem ser *smartphones, tablets*, ou interruptores tácteis. Podem existir dispositivos específicos que se tornam importantes para o funcionamento do sistema. Por exemplo, para efetuar a comunicação entre a infraestrutura de domótica e a rede de internet pode-se instalar um *Gateway* de comunicação.

3.2.4. Protocolos de comunicação

Existem no mercado inúmeros protocolos de comunicação específicos para aplicação em domótica. As suas caraterísticas diferem muito e podem ser mais fáceis ou mais difíceis de implementar. Dividem-se em dois tipos de protocolos, os de norma aberta, cujas regras são do conhecimento público e podem ser consultadas ou os protocolos proprietários dos quais apenas se verificam as aplicações em funcionamento. Como protocolo aberto temos o *KNX*, como protocolo proprietário temos o exemplo do *Insteon*.

3.3. Protocolos de comunicação: discussão e análise comparativa

Na Figura 13 [15], podemos ver, a amarelo, a localização, a nível mundial, da sede de alguns dos responsáveis por protocolos na área da domótica. Esta imagem evidencia bem a quantidade de protocolos existentes. Verifica-se que a maioria se localiza nos Estados Unidos e na Europa.

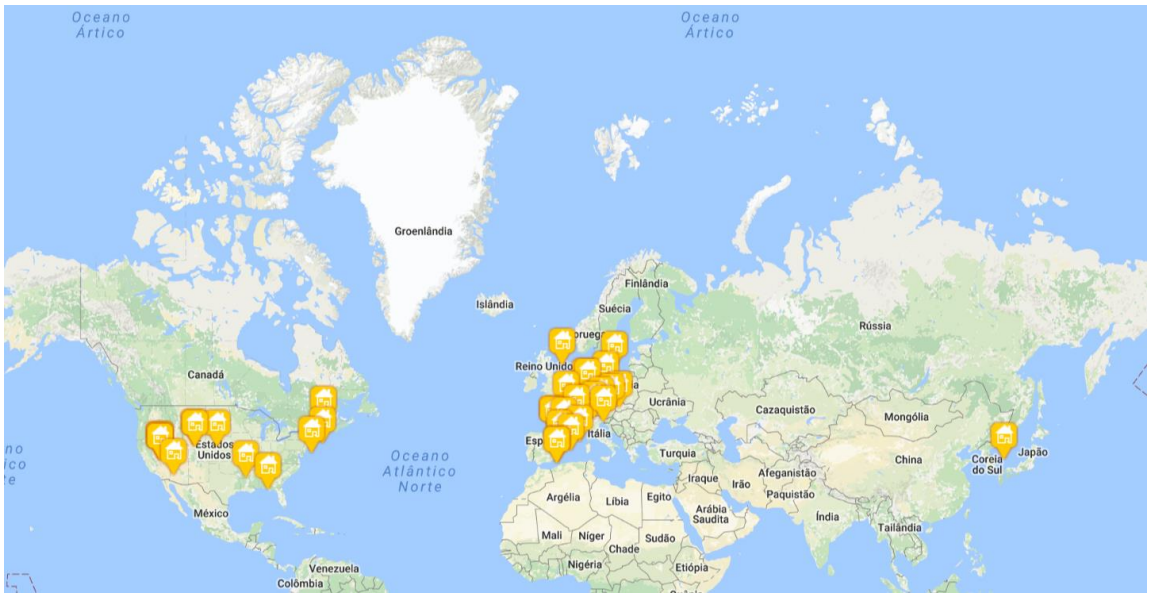


Figura 13: Sinalização, no mapa, da sede de alguns padrões de domótica a nível mundial.

De seguida serão analisados alguns dos protocolos mais utilizados em domótica.

3.3.1. O protocolo *X-10*

Este protocolo é usado para a transmissão de informação utilizando a corrente elétrica como onda portadora. Foi desenvolvido entre 1976 e 1978 pelos engenheiros da *Pico Electronics Ltd*, na Escócia. Utilizava baixa tensão, tanto monofásica como trifásica, a velocidades muito baixas (60 bits/s nos EUA e 50 bits/s na Europa). Tinha a vantagem de ter custos baixos pois utilizava a infraestrutura normal. É um protocolo que continua no mercado e é o mais utilizado nos EUA pois os equipamentos têm custos reduzidos e é de fácil implementação pois não necessita de conhecimentos técnicos especializados. Os dados são enviados a cada passagem por zero da onda de tensão alternada de uma fase através de comandos *standard*. Os transmissores enviam estes comandos por *broadcast*, precedidos pela identificação do dispositivo a ser atuado. Cada recetor está relacionado com uma identificação de unidade e só reage aos comandos que lhe são endereçados.

3.3.2. Protocolo *CEBus*

Em 1984 vários membros da *EIA (Electronics Industry Association)*, da América do Norte, quiseram alargar as funcionalidades na domótica para além das tradicionais que existiam *(ON, OFF, DIMMER xx, ALL OFF, entre outros*). Especificaram e desenvolveram o protocolo *CEBus (Consumer Electronic Bus)* e em 1992 apresentada a primeira especificação. Trata-se de um protocolo aberto, mas os fabricantes para poderem lançar produtos com esta certificação precisam de uma autorização da *CIC (CEBus Industry Council)*. É uma associação de diferentes fabricantes de software e hardware que certifica os novos produtos *CEBus*. Se o produto passar

as especificações, o fabricante paga uma taxa para puder utilizar o logotipo do protocolo. O protocolo utiliza vários meios de comunicação. A rede elétrica, o cabo entrelaçado, *Ethernet* e a radiofrequência.

3.3.3. Protocolo *LonWorks*

Lonworks Echelon apresentou a tecnologia *LonWorks* em 1992, desde então muitas empresas utilizam esta tecnologia para implementarem redes de controle distribuídas e automatização. Contempla quase todas as situações de controle, mas a sua utilização tornou-se mais comum em infraestruturas maiores como hotéis, devido ao seu custo embora apresente grande robustez e fiabilidade. Utiliza ligação ponto-a-ponto, o que significa que os componentes comunicam entre si, prevenindo o congestionamento de informação e falhas de comunicação. Esta técnica confere-lhe a sua robustez. Em termos de meios de comunicação utiliza o par entrelaçado, a rede elétrica, a fibra ótica e a radiofrequência.

3.3.4. Protocolo *KNX/EIB*

O protocolo *KNX* apareceu com a associação, do mesmo nome, que foi criada em 1999 e cuja sede se localiza em Bruxelas. Esta surgiu da fusão de três antigas associações europeias que já trabalhavam em protocolos de domótica, nomeadamente a *BCI* (França) que promovia o sistema *Batibus*, a associação *EIB* (Bélgica) que promovia o sistema *EIB* e, finalmente, da *European Home Systems Association* (Holanda) que promovia o sistema *EHS*. O protocolo surge virado para a domótica e pretende-se estabelecer como padrão europeu e mundial. Conta já com mais de 400 marcas associadas [16]. A Associação *KNX* também oferece suporte aos sistemas anteriores, o *Batibus*, o *EIB* e o *EHS*, incluindo a certificação de acordo com esses mesmos padrões. Como o *EIB* é compatível com o *KNX*, a maioria dos dispositivos pode ser rotulada tanto com o *KNX* como com o logotipo do *EIB* embora, atualmente, se comece a utilizar apenas a designação *KNX*. A arquitetura distribuída do protocolo *KNX* é ilustrado na Figura 14 [16].

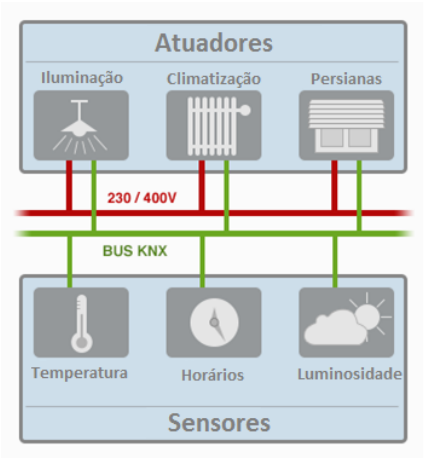


Figura 14: Esquematização de uma instalação distribuída que utiliza *KNX*.

O comando e controlo é feito à custa de dispositivos adequados que poderão ser programados de várias formas e, nos casos mais complexos, pode ser mesmo necessário utilizar um computador.

Um sistema *KNX* básico requer os seguintes constituintes: uma fonte de alimentação de 29 V DC para funcionamento dos dispositivos da instalação; os sensores, como interruptores, termostatos, estações meteorológicas, entre outros. que geram comandos, enviando esses mesmos comandos através de telegramas; e os atuadores que recebem os telegramas e realizam as ações. Esses telegramas são transportados através do barramento de comunicação.

A associação *KNX* é detentora da marca registrada *KNX*. Define os testes e padrões de qualidade através de grupos de trabalho e de especialistas e as caraterísticas do protocolo constam nas especificações *KNX*. De uma forma geral, os objetivos ao criar este protocolo foram:

Criar um único standard para a domótica e automação de edifícios que cubra todas as necessidades e requisitos das instalações profissionais e residenciais no âmbito europeu;

- Melhorar as prestações dos diversos meios físicos de comunicação sobretudo na tecnologia de radiofrequência, fundamental para a efetiva consolidação da domótica;

- Introduzir novos modos de funcionamento que permitam aplicar uma filosofia *plug-and-play* a muitos dispositivos típicos de uma casa;

- Envolver as empresas fornecedoras de serviços como as de telecomunicações e de eletricidade, com o objetivo de desenvolver a telegestão nas casas.

Atualmente, o protocolo *KNX* está aprovado como:

- *International Standard (ISO/IEC14543-3);*

- *European Standard (CENELEC EN50090 e CEN EN 13321-1 e 13321-2);*

- *Chinese Standard (GB/Z 20965);*

- *ANSI/ASHRAE Standard (ANSI/ASHRAE 135).*

Na Tabela 2, constam os protocolos mencionados, o tipo, isto é, abertos ou fechados e o meio físico que utilizam.

Tabela 2: Exemplos de protocolos, tipo e respetivos meios de comunicação.

Protocolo	Tipo	Meio físico
X-10	Aberto	Rede Elétrica
Lonworks	Aberto	Rede elétrica, Barramento cablado
KNX	Aberto	Par Entrelaçado, Rede Elétrica, RF , IR, *Ethernet*
CEBus	Aberto	Par E*ntrelaçado*, Rede Elétrica, RF, IR, *Ethernet*
Insteon	Proprietário/Fechado	Rede elétrica e RF

3.4. Vantagens do protocolo *KNX* face a outros protocolos

Existem muitos outros protocolos, mas devido à pouca representatividade no mercado não foram analisados. Dos protocolos analisados, o protocolo *KNX* tem hoje em dia, no mercado mundial, mais de 400 fabricantes em 33 países que fabricam produtos, que podem ser instalados numa mesma instalação garantindo-se a seu funcionamento. Este facto permite que se possam adquirir produtos de diferentes fabricantes com uma compatibilidade garantida, podendo-se utilizar como critério o preço do produto. Trata-se de um protocolo distribuído e, portanto, fiável. É de grande escalabilidade e, por este motivo, o *KNX* pode ser utilizado tanto em pequenos projetos como em grandes projetos, por exemplo, escolas, hotéis, ou outros mais complexos. Outra caraterística importante é o facto da associação *KNX* disponibilizar, gratuitamente, o software para se trabalharem com até 5 dispositivos *KNX*. Salienta-se que a licença profissional é dispendiosa e este é um aspeto negativo. Outra vantagem, face a outros protocolos, é o facto de se puderem utilizar vários meios de comunicação, por exemplo, par entrelaçado, rádio frequência ou *Ethernet*. Os dispositivos, como são certificados, são obrigados a ter recuperação depois de uma falha de corrente, isto é, os dispositivos podem ser configurados, para manterem os mesmos estados, após um corte de luz. O barramento auxiliar, único, deste protocolo permite ligar conforto, comunicações, energia e segurança de uma instalação, na mesma rede pois é um protocolo fortemente representado no mercado e com inúmeras soluções para a interligação das diferentes partes a nível residencial. Por estes motivos este será o protocolo estudado e utilizado na validação experimental.

Capítulo 4 – Análise e funcionamento do protocolo *KNX*

4.1. Análise do protocolo *KNX*

Este protocolo foi desenvolvido para estar desagregado de qualquer plataforma de hardware específica, quer isto dizer que as diferentes partes do sistema trabalham de forma independente e, se uma das partes deixar de funcionar, trata-se de um tipo de protocolo distribuído. Os dispositivos *KNX* para poderem operar têm de ser configurados. Estes podem ser configurados de duas maneiras diferentes em função da complexidade da instalação ou da experiência do instalador.

4.1.1. Configuração dos dispositivos *KNX*

Os modos de configuração dos dispositivos são os seguintes [17]:

O modo *"E-Mode" (Easy Mode)* adequado para instaladores com menos conhecimento em *KNX*. Normalmente os dispositivos, que permitem este modo, vêm pré-programados de forma a comunicarem entre si e são apenas necessárias algumas operações para adequar os dispositivos aos requisitos do utilizador final. Este tipo de configuração é, normalmente utilizada apenas em pequenos projetos.

O modo *"S-mode" (System Mode)*, corresponde a um modo de operação em que os dispositivos têm de ser programados e instalados a partir de um computador com o programa denominado *ETS (Engineering Tool Software)* que tem de ser instalado. A utilização deste software requer a instalação prévia da base de dados dos produtos *KNX* utilizados. Este modo destina-se a pequenas e grandes instalações. Todos os passos de configuração têm de ser efetuados manualmente pelos programadores / instaladores e é o método mais utilizado pelos projetistas e instaladores *KNX* certificados.

4.2. Meios de comunicação no protocolo *KNX*

O meio de transmissão mais comuns é o cabo (par entrelaçado), no entanto este protocolo permite a comunicação pela rede elétrica (*PowerLine*), rádio frequência e por *IP* (*Ethernet*). Em termos de utilização dos diferentes meios, neste protocolo temos:

- Par de condutores (*TP*1): que aproveita a norma *EIB* equivalente.

- Par de condutores (*TP*0): que aproveita a norma *Batibus* equivalente.

• Corrente elétrica (*PL*100): que aproveita a norma *EIB* equivalente.

• Corrente elétrica (*PL*132): que aproveita a norma *EHS* equivalente.

• *Ethernet*: utiliza a norma *KNXnet/IP*.

• Radiofrequência: que aproveita a norma *EIB.RF*.

• Existe também o *EIB*.IR que transmite o sinal por infravermelho, até uma distância máxima de cerca de 12 metros. É normalmente utilizado como meio intermediário entre os meios anteriores e dispositivos que recebem sinais de IV, por exemplo televisões, aparelhos de ar condicionado, entre outros.

Na Tabela 3 estão resumidas as áreas preferenciais de utilização para cada um dos meios. Sempre que são realizadas obras de raiz opta-se pelo cabo, o par e*ntrelaçado*, devido às caraterísticas que permitem uma maior velocidade de transferência de dados.

Tabela 3: Meios de transmissão de dados utilizando o protocolo *KNX*.

Meio	**Meio de Transmissão**	**Áreas de Utilização Preferencial**
Par E*ntrelaçado* (*Twisted Pair*)	Cabo dedicado	Novas construções ou remodelações profundas das instalações. Onde são transferidas grandes quantidades de dados de comunicação.
Rede Elétrica (*PowerLine*)	Cabos elétricos	Em locais onde um cabo de barramento não existe, mas existe um cabo de alimentação de 230 V.
Rádio Frequência	Rádio	Em locais onde não existe cablagem ou onde não é desejada essa mesma cablagem.
IP	*Ethernet*	Em grandes instalações onde é necessária uma estrutura de interligação.

São várias as normas (Tabela 4), em vigor, em função do tipo de meio.

Tabela 4: Normas relativas aos diferentes meios de transmissão de dados em *KNX*.

Meio de comunicação / Norma
Par entrelaçado 1 (*TP*1): usa a norma *EIB* equivalente.
Par entrelaçado 0 (*TP*0): usa a norma *EHS* equivalente.
Ondas portadoras (*PL*110): usa a norma *EIB* equivalente.
Ondas portadoras (*PL*132): usa a norma *EHS* equivalente.
Ethernet: usa a norma *EIB.net*
Radiofrequência: usa a norma *EIB*.RF

Na prática, o tipo de meio utilizado e a norma utilizada traduz-se em diferentes velocidades de transmissão de dados, Figura 15 [18].

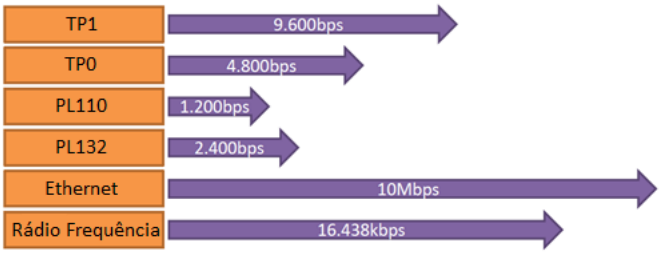


Figura 15: Normas de transmissão de dados e respetiva velocidade de transmissão.

4.2.1. Par entrelaçado (*TP*) no *KNX*

O meio físico mais utilizado atualmente em *KNX* e o par entrelaçado *TP*1. Este permite a injeção de tensão nos componentes, a partir da fonte de alimentação de tipicamente 30V, e a simultaneamente, a transferência de dados no sistema entre os componentes. Este meio permite o envio de telegramas *KNX*/*EIB*, no modo de impulsos binários, em série. Cada octeto do telegrama é enviado para o barramento *TP* utilizando este modo *bit* a bit. Cada octeto está incluído num caractere mais completo que é constituído por 13 bits. O *bit* inicial, seguido dos oito *bits* do octeto, um *bit* de paridade par para controlo de erros, um *bit* de identificação do fim do caractere série e dois *bits* de pausa. De seguida é enviado outro octeto, do mesmo modo, e assim sucessivamente até ser enviado um telegrama, em modo assíncrono em que o tempo de duração da transmissão de cada *bit* é de 104 µs, tal como se descreve na Figura 23 [17].

4.2.2. Rede elétrica em *KNX*

A utilização da rede elétrica (230 V / 50 Hz), existente num edifício ou para expansão de uma infraestrutura, facilita uma instalação de domótica uma vez que não é necessário nenhum cabo adicional. Deve-se apenas utilizar uma das três fases da linha e os dados do protocolo são sobrepostos à tensão da rede. O *KNX* tem duas especificações para este meio físico que são o *PL*110 e o *PL*132 herdados de dois protocolos anteriores que se fundiram, mas cujas normas foram adotadas. O *PL*110 tem uma taxa de transferência de 1200 bits/s e provém do *EIB* pelo que dispositivos *EIB PL*110 podem comunicar com dispositivos *KNX*/*EIB PL*110. O *PL*132 tem uma taxa de transferência superior, isto é, de 2400 bits/s e foi adotado do *EHS* que ainda o utiliza, no entanto, estes dispositivos não podem comunicar entre si porque utilizam protocolos diferentes. Para enviar sinais digitais utiliza-se modulação em frequência, mais especificamente, modelação por comutação em frequência pois adicionam-se duas frequências fixas à frequência da rede e denomina-se *Spread frequency Shift Keying* (*SFSK*). A frequência para o valor lógico um é de 115,2 kHz e para o valor lógico zero é de 105,6 kHz. Para o protocolo

*PL*110 a duração de um *bit* é de 833,33 µs. Na Figura 16 pode-se ver um exemplo de sinal transmitido em *PL* [19] [17] [20].

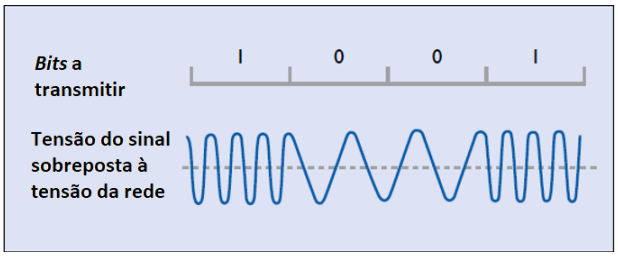


Figura 16: Modulação em frequência: frequência do sinal com a frequência da rede.

A potência do sinal transmitido tem de ser muito baixa para não afetar a qualidade do sinal da rede.

4.2.3. Rádio Frequência e Infravermelhos em *KNX*

Quando a utilização por cabo não é possível, o *KNX* permite a utilização ondas eletromagnéticas para comunicação. Na norma *KNX* RF estão definidos dois tipos de redes para transmissão dos dados que são, a rádio frequência (RF) e os infravermelhos (IV). Existem duas versões de *KNX* RF que são *KNX* RF *ready* e *KNX* RF *Multi*. O primeiro transmite os telegramas através de ondas de rádio na banda de frequência de 868 MHz, ou seja, só tem um canal de comunicação. Isto pode ser um problema pois se surgiram interferências na rede a comunicação é difícil ou impossível e, portanto, o sistema fica vulnerável. A segunda solução mais fiável, pois, os dispositivos podem comunicar em várias bandas, comutando automaticamente de uma para outra, se a primeira estiver ocupada. Neste protocolo existem canais rápidos e lentos. Os canais lentos foram pensados para dispositivos que necessitam de estar sistematicamente no modo recetor como é o caso de sistemas *HVAC*. Nos sistemas rápidos a velocidade de transferência de dados pode chegar aos 16384 kbps. Existem dispositivos que suportam a comunicação bidirecional e outros unidirecional. Normalmente, os dispositivos unidirecionais são alimentados por pilhas ou baterias pois têm consumos significativamente mais baixos que os bidirecionais que devem estar sempre no modo de receção. Estes, por norma, estão ligados à rede elétrica de 230 V. A modulação dos sinais em rádio frequência utiliza uma modulação idêntica à *PL*, embora o meio seja diferente, isto é, é do tipo *Frequency-shift keying (FSK*) ou modulação por comutação da frequência. Devido ao meio físico ser aberto, e consequentemente, haver uma maior probabilidade de cruzamento com redes vizinhas, é necessário alterar o domínio dos endereços *KNX* para endereços maiores. Estes endereços maiores utilizam a combinação de endereços *KNX* com o número de série de cada emissor/recetor de RF. Com esta solução garante-se que o endereço é único. Os aparelhos de RF recentes são sempre compatíveis com as duas normas *KNX* RF. Por outro lado, os infravermelhos, são um tipo de meio de comunicação normalmente utilizado nos comandos de

infravermelhos que permitem controlar dispositivos *KNX ou a partir de dispositivos KNX controlar outros dispositivos do meio como por exemplo televisões*. São utilizados em distâncias pequenas, na ordem de poucos metros, devido às caraterísticas desta radiação. Esta radiação não contorna meios opacos pelo que só consegue percorrer pequenas distâncias e por isso normalmente são utilizadas em meios confinados. A especificação da utilização de infravermelhos, como meio de comunicação, está definida na norma *EIB* que foi transposta para a norma *KNX*. Os infravermelhos são normalmente utilizados no envio de telegramas *KNX*, para dispositivos que contêm um recetor de infravermelhos, e que funcione como um *Gateway*, para passar os telegramas para o meio físico *TP*1 ou vice-versa para comandar uma televisão a partir da rede *KNX*. A transmissão de dados por infravermelhos é assíncrona e pode ser unidirecional ou bidirecional, mas só ocorre em *half-duplex*. A frequência do sinal que é emitido pelo emissor de infravermelhos é de 447,5 *kHz* mas, neste caso é utilizada um tipo de modulação é em amplitude com uma taxa de transferência de aproximadamente 7000 *bits/s*. Os endereços *KNX* utilizados são os endereços *KNX/EIB* normais [17] [20].

4.2.4. *Ethernet*

Este meio físico, ao contrário dos anteriores, não tem nenhum documento na norma que o especifique uma vez que é uma rede de comunicação aberta com especificações segundo o *IEEE*. É utilizada normalmente como rede local em conjunto com a Internet. O meio físico utilizado é Ethernet sobre o protocolo de rede *IP*. O *KNX*, referencia uma norma, herdada do *EIB*, a *EIB.net*, que permite a utilização do *KNX* sobre redes *TCP/IP*. A norma é denominada por *KNXnet/IP*. A utilização deste meio físico ocorre com a ligação a outro meio físico como por exemplo o *KNX TP*1. A norma *KNXnet/IP* define um servidor que funciona como um *Gateway* e que interliga a rede *KNX*/EIB a uma rede *IP* [21].

4.3. Topologia no *KNX* - Par entrelaçado (*TP*1)

A topologia de uma instalação está relacionada com a estrutura disposta na implementação do projeto, esta pode ser disposta em áreas, linhas e segmento de linha [17].

4.3.1. Segmento de linha

O segmento mais pequeno na topologia *KNX* é o segmento de linha. Consiste no acoplamento de uma fonte de alimentação adequada, com um máximo de 64 dispositivos, ao barramento.

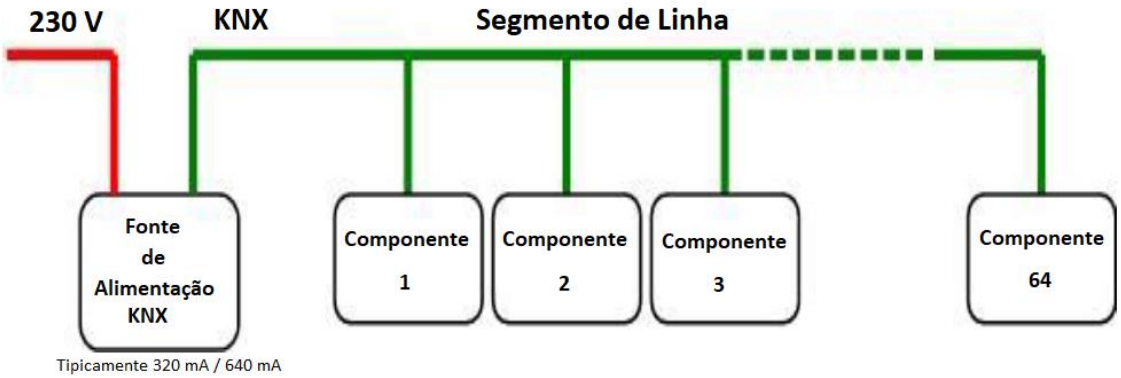


Figura 17: Estrutura mínima em *KNX*.

4.3.2. Linha

O segmento seguinte é uma linha que consiste no acoplamento de um máximo de 4 segmentos de linha, podendo obter-se até um máximo de 256 dispositivos do barramento, por linha, incluindo os amplificadores, dispositivos necessários para o acoplamento dos 4 segmentos, Figura 18, que devem ser colocados paralelamente entre si [18].

4.3.3. Área

No caso de se utilizarem dispositivos em mais do que uma linha, devem acoplar-se a uma linha principal. Para este efeito utiliza-se um acoplador de linha. Este conjunto denomina-se área. Numa área podem-se acoplar até um máximo de 15 linhas, Figura 18.

4.3.4. Linha de Área *(BackBone)*

Para o caso de se utilizar mais do que uma área, a ligação entre as mesmas, é feita por uma ligação chamada linha de áreas ou *backbone*. Para a ligação entre áreas é necessário um acoplador de áreas. O número máximo de áreas que se podem ligar é de 15, Figura 18 [22].

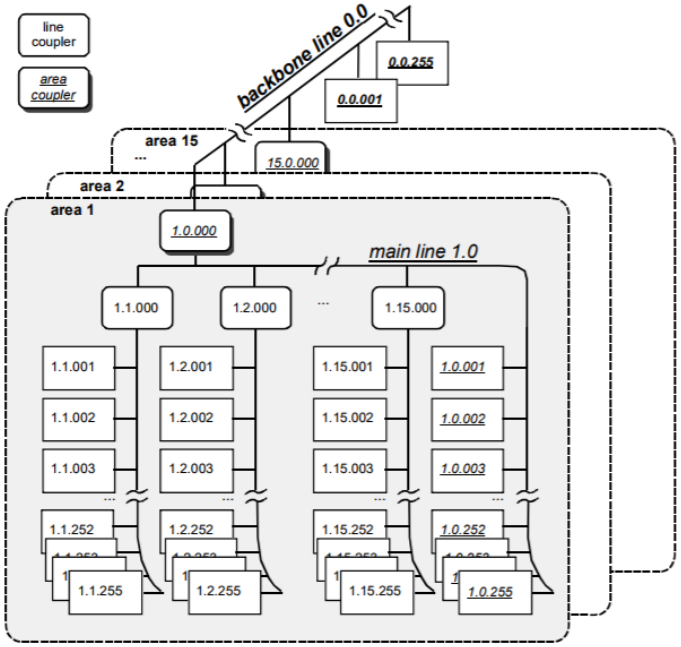


Figura 18: Estrutura geral em *KNX*.

Em síntese, os componentes físicos necessários, para ligar toda a estrutura *KNX*, resumem-se a 3 tipos:

Acopladores de área (na Figura 19 [18] representado por AA), têm por função unir uma área com a linha principal de áreas.

Acopladores de linha (na Figura 19 representado por AL), têm por função unir uma linha com a linha principal.

Amplificadores de linha (na Figura 19 representado por AmpL), têm por função unir dois segmentos de linha.

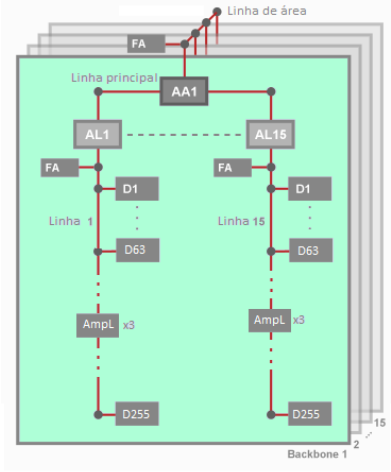


Figura 19: Estrutura com a identificação dos componentes de ligação.

Relativamente ao tipo de ligação do barramento, podem-se utilizar diferentes configurações (topologias), tipicamente são em linha, estrela, anel e/ou árvore, como é mostrado na Figura 20. A ligação mista é possível, devendo-se sempre respeitar as polaridades do par utilizado no *KNX* (vermelho e preto) [18].

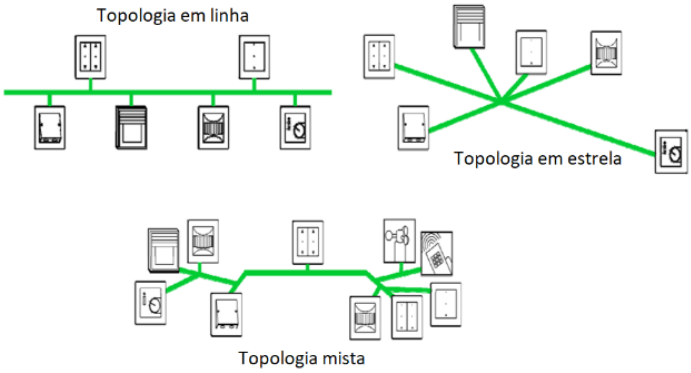


Figura 20: Tipos de ligação do barramento, utilizadas na topologia *TP*1.

4.4. Configuração dos componentes, no protocolo *KNX*

Para puderem comunicar os componentes ligados no barramento, devem ser configurados para serem reconhecidos. É obrigatório a atribuição de um endereço individual que identifica cada componente, e endereços de grupos, que são utilizados pelo protocolo para o funcionamento normal da instalação [17].

4.4.1. Endereço individual

Cada dispositivo deve ter um endereço individual que é único. Este endereço tem o seguinte formato: Área [4 bit] - Linha [4 bit] – Dispositivo [1 *byte*]. O primeiro número corresponde à área onde se encontra o dispositivo do barramento. Podem ser atribuídos os números de 1 a 15 uma vez que são as áreas possíveis respetivamente. A este número pode atribuir-se o 0 (zero). Indica que temos um componente na linha de áreas. O segundo número indica a linha e, o número atribuído pode variar de 1 a 15, que são o número de linhas disponíveis por área. A atribuição do número 0 (zero) indica que temos pelo menos um dispositivo na linha principal. Finalmente, o terceiro e último número pode variar entre 1 e 255. O número zero, se estiver atribuído, refere-se a um acoplador de linha ou de área. Na Figura 21, representa-se esquematicamente um endereço genérico [17] [20].

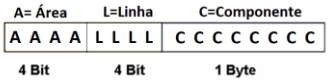


Figura 21: Direção Física em *KNX*.

O dispositivo normalmente recebe este endereço através de um botão de programação em que, após pressão do mesmo, os dipositivos mantêm um LED aceso enquanto a programação é efetuada e o endereço individual é adicionado ao dispositivo. Este endereço é utilizado para os seguintes propósitos: diagnóstico, deteção de erros, modificação da instalação por reprogramação. Endereçamento dos objetos de interface usando ferramentas de inicialização ou outros dispositivos. No entanto, o endereço individual não tem qualquer significado durante o funcionamento normal da instalação.

4.4.2. Endereço de Grupo

A comunicação entre os dispositivos, numa instalação, realiza-se através de endereços de grupo. A configuração do endereço de grupo via *ETS*, pode ser livre, isto é, um nível, dois níveis (grupo principal / subgrupo) ou com uma estrutura de 3 níveis (grupo principal / grupo intermediário / subgrupo) que é a mais utilizada. A estrutura dos níveis pode ser alterada nas propriedades do projeto, no *ETS*, em cada projeto individual. O endereço do grupo 0/0/0 é reservado para as chamadas mensagens de difusão (*Brodcasts*, telegramas para todos os dispositivos de barramento disponíveis). O projetista ou engenheiro, no *ETS*, decide qual deve ser a estrutura de níveis usados, que tem de ser mantida até ao final do projeto. Também define cada uma das funções, por exemplo (comutação, *dimmer*, entre outros). Na Figura 22 [20] mostra-se um exemplo do número de níveis escolhidos e a estrutura do endereço do grupo respetivo, em cima uma estrutura com três níveis, ao centro com dois e em baixo uma estrutura com um nível [20].

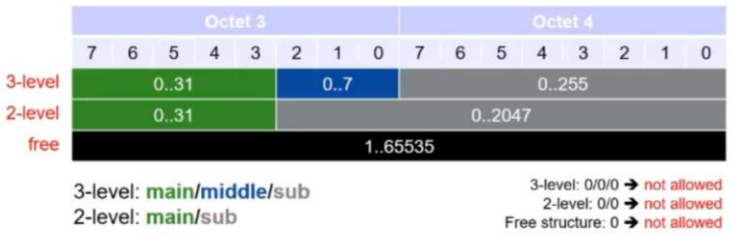


Figura 22: Direção de Grupo.

Cada endereço de grupo pode ser atribuído aos dispositivos de barramento conforme necessário, independentemente de onde se encontra o dispositivo no sistema. Os atuadores podem ler vários endereços de grupo, no entanto, os sensores só podem enviar um endereço de grupo em cada telegrama. Os endereços de grupo são atribuídos aos objetos de comunicação dos respetivos sensores e atuadores, criados e atribuídos, com a ajuda do *ETS*, no "*S-modo*" ou automaticamente e invisíveis ao utilizador no "*E-mode*". Quando se utilizam os grupos principais 14 e 15 no *ETS*, deve-se ter em conta que estes endereços de grupo não são filtrados por acopladores *TP*1 e, portanto, pode-se influenciar negativamente a dinâmica de toda a instalação. O número de endereços de grupo que podem ser atribuídos a um sensor ou atuador

é variável e depende do seu tamanho da memória. Na Tabela 5, temos o exemplo da atribuição de três endereços de grupo adicionados com uma estrutura de 3 níveis [19].

Tabela 5: Exemplos de 3 direções de grupo atribuídas no *ETS*.

Grupo principal	Grupo Intermedio	Subgrupo	Direção de grupo
1: Iluminação	2: R/C	1: Corredor	1/2/1
		2: Garagem	1/2/2
2: Persianas	3: 1º Andar	1: Escritório	2/3/1

4.4.3. Objetos de Comunicação

Os objetos de comunicação *KNX* são locais da memória nos dispositivos do barramento. O tamanho destes objetos varia entre 1 *bit* e 14 *bytes*. O tamanho dos objetos de comunicação depende da sua função. Por exemplo, para a comutação de uma lâmpada são necessários dois estados (0 e 1) e são utilizados objetos de comunicação de 1 bit. Os dados envolvidos na transmissão de texto são mais complexos e os objetos de comunicação têm de ter um tamanho máximo de 14 *bytes*. No entanto o *ETS* só permite ligar objetos com o mesmo tamanho usando endereços de grupo. Vários endereços de grupo podem ser atribuídos a um objeto de comunicação, mas apenas um é o endereço de grupo de envio [19] [17].

O valor de um objeto é enviado no barramento da seguinte maneira:

A) Se, por exemplo, se pressiona um botão, o sensor de comutação marcará um "1" para o seu objeto de comunicação. À medida que a sinalização de comunicação e de transmissão é definida para este objeto, este dispositivo enviará um telegrama, através do barramento, com a informação, “Endereço de grupo, por exemplo, 1/1/1, escrever valor, 1".

B) Todos os dispositivos de barramento, em toda a instalação *KNX*, que também tenham o mesmo endereço de grupo (1/1/1) escreverão então "1" no próprio objeto de comunicação.

C) O software aplicativo do atuador estabelece que o valor neste objeto da comunicação foi alterado e executa o processo de comutação.

4.4.4. *Flags*

Cada objeto de comunicação tem sinalizadores, chamadas *Flags* (Bandeiras), que são utilizados para definirem propriedades. Estas *Flags* podem ser ativadas ou desativadas no *ETS* e mudam a forma de funcionamento final dos dispositivos. Estas estão descritas na Tabela 6 [17]:

Tabela 6: Flags em *KNX*.

Comunicação *(COMMINICATION)*	Opção ativada	O objeto de comunicação tem uma comunicação normal como barramentos.
	Opção desativada	É acusado a receção de telegramas, mas o objeto de comunicação não muda.
Leitura *(READ)*	Opção ativada	O valor do objeto de comunicação pode ler-se (consultar-se) desde o barramento.
	Opção desativada	O objeto de comunicação não se pode ler desde o o barramento.
Escrita *(WRITE)*	Opção ativada	O valor do objeto de comunicação pode modificar-se desde o barramento.
	Opção desativada	O valor do objeto não pode alterar-se através do barramento.
Transmissão *(TRANSMIT)*	Opção ativada	Se houve uma alteração num objeto, será transmitido o valor correspondente.
	Opção desativada	O objeto transmite só um telegrama de resposta em caso de pedido de leitura.
Atualização *(UPDATE)*	Opção ativada	Os telegramas de resposta com informação do valor são interpretados como ordens de escrita. Atualiza-se o valor do objeto de comunicação (Habilitado por defeito nos objetos *System* 1).
	Opção desativada	Os objetos de resposta com informação do valor não são interpretados como ordens de escrita. O valor do objeto de comunicação continua inalterado.
Leitura com inicialização *(READ ON INIT)*	Opção ativada	O aparelho envia autonomamente ordens de leitura de valores para a inicialização do objeto de grupo correspondente depois de voltar a tensão (disponível só com determinadas máscaras).
	Opção desativada	Com o retorno da tensão, o componente não inicia o valor do objeto do grupo assignado mediante ordens de leitura de valores.

Capítulo 5 – Protocolo *KNX*: comunicação

5.1. Telegramas *KNX*

Um telegrama gera-se quando ocorre um acontecimento em pelo menos um dos dispositivos do barramento, por exemplo, quando se utiliza um botão de pressão. O componente gera e envia um telegrama através do barramento de comunicação. Estes telegramas são fundamentais para comunicação entre os dispositivos e são parametrizados para uma garantia de compatibilidade entre os mesmos (ex.: em *dimmers* ou relógios) e entre fabricantes. A sua transmissão ocorre depois de o barramento ficar desocupado um período t1 que corresponde ao tempo de 50 *bits*. Finalizada a transmissão do telegrama, os componentes do barramento utilizam o tempo t2, correspondente ao tempo de 13 *bits*, para verificarem se o telegrama foi recebido corretamente. Todos os componentes do barramento, visados, enviam uma resposta "ACK" simultaneamente. O tempo de envio de um telegrama varia entre os 20 e os 40 ms, em função dos dados úteis do telegrama, que podem aumentar o tamanho do mesmo. Em *TP*1 o telegrama é transmitido a uma velocidade de 9600 *bits/s*, ou seja, um *bit* ocupa o barramento durante 1/9600 segundos, ou seja, os 104 μs referidos no capítulo anterior. A Figura 23 [18] mostra um diagrama temporal de um telegrama *KNX* em *TP*1 [17].

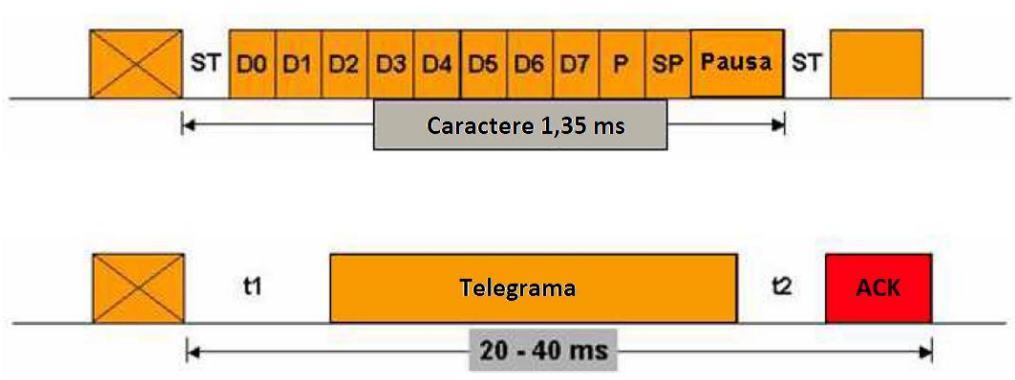


Figura 23: Diagrama temporal *KNX* em *TP*1 de um caractere e de um telegrama.

O telegrama não tem no cabeçalho qualquer referência relativa ao meio físico pelo que é independente destes. Se juntarmos todos os carateres que constituem um telegrama temos a estrutura da Figura 24 [17] [22].

octet 0	1	2	3	4	5	6		7	8	..	N - 1	N ≤ 22
Control Field	Source Address		Destination Address		Address Type; NPCI; length	TP CI	AP CI	data /APCI	data			Frame Check

Figura 24: Estrutura de um telegrama *KNX*.

Um telegrama é formado por quatro campos, eles são, o campo de controle (octeto 0), campo de direção (octeto 1 a 6), campo de dados (octetos 7 mais até 16 *Bytes*) e campo de verificação (o último octeto). O campo de dados pode variar de comprimento os restantes são campos de comprimento fixo. A informação transmite-se na totalidade na forma de carateres de 8 bits, octetos. O último campo que consta nos telegramas é o dos dados de deteção de erros /controle, que garantem um nível de fiabilidade nas transmissões extremamente elevado [17] [22].

5.1.1. Estrutura de um telegrama *KNX*

O Campo de Controle (*Control field*) Figura 25 [20], indica a prioridade que um determinado telegrama tem quando é enviado pelo dispositivo no barramento (alarme, serviços do sistema ou serviços comuns). Define ainda se um telegrama é normal ou se é estendido. Os telegramas estendidos não são utilizados, mas, a norma deixa em aberto este tipo de telegramas para utilizações futuras. Por este motivo não se define a norma para este tipo de telegrama [17].

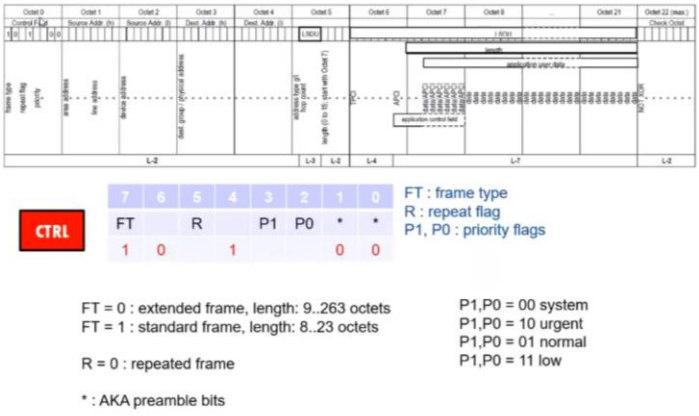


Figura 25: 1º octeto que corresponde ao campo de controle.

A Direção do Emissor *(Source address)*, Figura 26 [20], indica a direção física do dispositivo que envia o telegrama (4 *bits* para a área, 4 *bits* para a linha e 8 *bits* com o número do dispositivo).

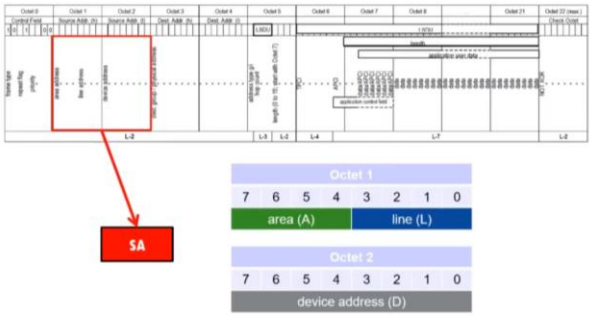
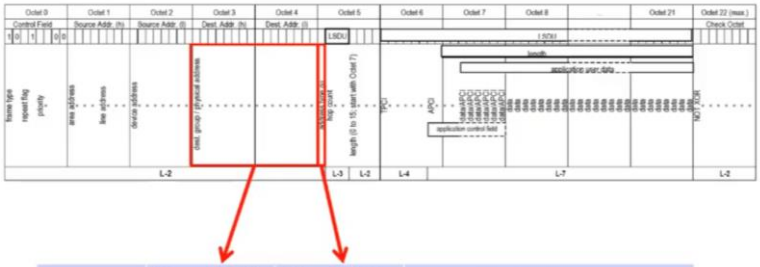


Figura 26: Endereço do emissor, octetos 2 e 3 do telegrama.

A Direção de Destino (*Target address*) Figura 27 [20] pode ter dois significados, uma direção física ou um endereço de grupo. Depende do valor que tenha o campo do *bit* mais significativo. Se tiver o valor "0" trata-se de uma direção física e o telegrama é enviado exclusivamente a um dispositivo. Se tem o valor "1" trata-se de uma direção de grupo e o telegrama dirige-se a todos os dispositivos que tenham essa direção de grupo. Se a direção de grupo for a 0/0/0 trata-se de uma comunicação em *broadcast*, isto é, é um telegrama transmitido para todos os dispositivos da rede [17].



	DA - 16 bit	AT - 1 bit	Service type
broadcast	0/0/0	1	network management
multicast	GA	1	runtime
unicast	IA	0	device management

Figura 27: Direção do destino que pode ser uma direção física ou direção de grupo.

A transferência de telegramas pode ainda ser *multicast* e *unicast*. *Multicast* é transferida para vários dispositivos e *unicast* é uma transmissão ponto a ponto, ou seja, para um dispositivo. A Figura 28 [20] mostra as diferentes possibilidades de transferência de telegramas e alguns exemplos [17].

	DA	AT	service type	communication type	example
broadcast	0/0/0	1	network management	connectionless -> to all	IndividualAddrWrite
multicast	GA	1	runtime	connectionless -> to a group	GroupValueWrite
unicast	IA	0	device management	Connection-oriented -> to one device	MemoryWrite

Figura 28: Exemplos de comunicação com os octetos 3, 4 e *bit* de maior peso do octeto 5.

O Contador (*Routing, HC* de *Hop Count*), Figura 29 [20], utiliza-se para funções de roteamento, contando o número de saltos que um determinado telegrama efetua nos acopladores e repetidores. Cada vez que um telegrama passa num destes componentes é decrementado um valor. O Comprimento (*Lenth, LEN*), nos seus quatro *bits* indica-se quantos *bytes* extra tem o campo de dados denominado *PAYLOAD (*corresponde ao octeto 6 + os *bytes* extra). O valor 1

corresponde a um *Byte* e o valor 15 corresponde a 15 *Bytes* extra que são o número de *Bytes* máximos que podem seguir num telegrama *TP1*. Este campo contem o tipo de comando e os dados úteis do telegrama denominados *DTP* [17].

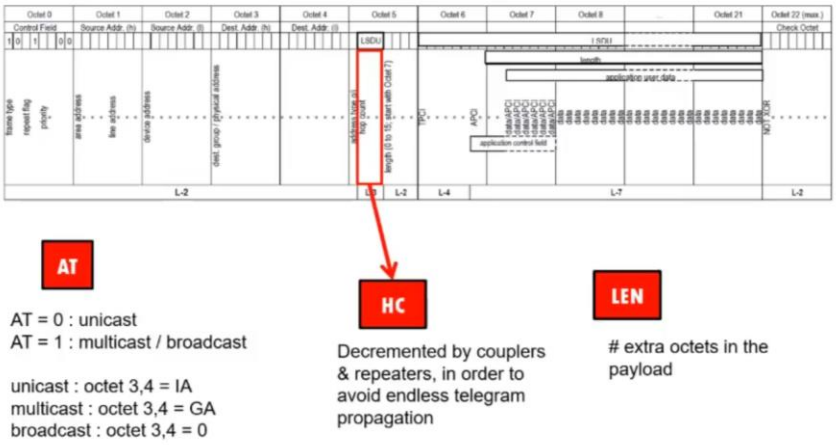


Figura 29: Octeto 5 para além do tipo de comunicação (AT), contém o HC, e LEN.

O *Byte* de Verificação (*Check Byte*), consiste num *byte* que se obtém do cálculo da paridade para todos *bytes* anteriores incluídos no telegrama. Quando um dispositivo recebe o telegrama, verifica se este está correto a partir do *byte* de controlo. Se a receção estiver correta, envia-se um reconhecimento, caso contrário envia-se um não reconhecimento, "*NACK*", para que o emissor repita o envio. Se o dispositivo está ocupado envia um código "*BUSY*" para que o emissor tente a transmissão com um pequeno atraso. Na Figura 30 [18] temos o exemplo da verificação de paridade cruzada que o protocolo utiliza. A soma dos *bits* do octeto com o *bit* de paridade deve verificar a paridade par, isto é, a soma deve ser zero. E a soma dos *bits* de igual peso de todos o telegrama deve verificar a paridade impar, isto é, a doma de todos os *bits* de igual peso com os *bits* de paridade, S7 a S0 na figura, devem ter o valor 1 [17].

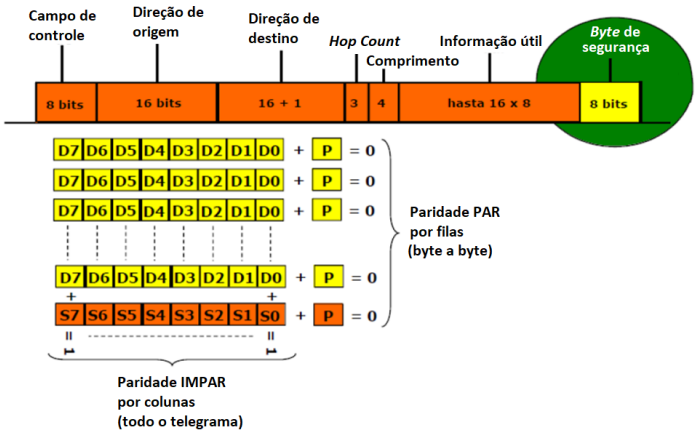


Figura 30: *Byte* de verificação

5.1.2. Receção de telegramas

O componente do barramento ou os componentes do barramento respondem com *byte* de verificação (*Check Byte*) do telegrama, para assegurar a receção correta da informação e, de acordo com esta, devolver uma resposta de confirmação "*ACK*". Se a receção não for correta é enviado uma mensagem *"NACK"* e repete-se até três vezes. Se o barramento está ocupado recebe uma mensagem com um "*BUSY*" e espera um tempo curto para enviar de novo o telegrama. Se o componente emissor não receber informação sobre um telegrama envia-o novamente, até três vezes, para depois interromper a transmissão [17].

Figura 31: Resposta do(s) dispositivos aos telegramas recebidos.

5.1.3. Dados úteis do telegrama (*Datapoint Types Standars: DTP*)

Para ocorrer uma alteração, nos dispositivos *KNX*, é necessário um comando adequado. Esta informação está incluída nos telegramas, no campo de dados, e o seu tamanho depende do tipo de comando. Estes comandos, incluídos nos telegramas, são os dados úteis e denominam-se *Datapoint Types Standars* (*DTP*) uma vez que também têm formato e estrutura dos objetos de comunicação para cada tarefa dos dispositivos no barramento. Permitem executar uma função, por exemplo, alterar o estado de um atuador ou simplesmente ler informação, como a hora, temperatura, ou dados dos dispositivos. A combinação de diferentes *DTP* tem o nome de Bloco Funcional. A designação de um *DTP* refere-se à função para que foi desenvolvido, ou seja, o mesmo *DTP* não fica restringido a uma área de aplicação. Um exemplo pode ser o *DTP* do tipo de percentagem, representado na norma *KNX* por 5.001, não serve só para regular um valor de iluminação num *dimmer* mas, pode ser utilizado para adequar a posição de uma válvula. Existem vários *DTP*, pois são enormes as potencialidades do Protocolo *KNX*. Um *DTP* para Acender / Apagar é do tipo 1.001, 1.002 para lógica booleana, e ativar, um *DTP* 1.003. A lista completa pode ser consultada na página *web* oficial da Associação *KNX*. Exemplificando apenas o caso mais simples, o tipo 1.001, a Figura 32, mostra em cor de laranja, o formato do *DTP*, neste caso, são necessários 2 *Bytes* que é o tamanho mínimo possível de um *DTP*. Para o comando "escrever", onde "cccc" têm o valor 0010, o último *bit* à direita contém um "1" ou um "0" para "Ligar" ou "Desligar", respetivamente. O comando "*read*", com "cccc" a valores 0000, solicitaria que o dispositivo de grupo endereçado informe sobre o seu estado, por exemplo ligado, desligado. Neste caso, a resposta seria uma mensagem de 1 bit. Noutros casos, a

resposta, poderia ser maior uma vez que o comprimento dos dados depende do tipo de *DTP* utilizado [17] [21] [23].

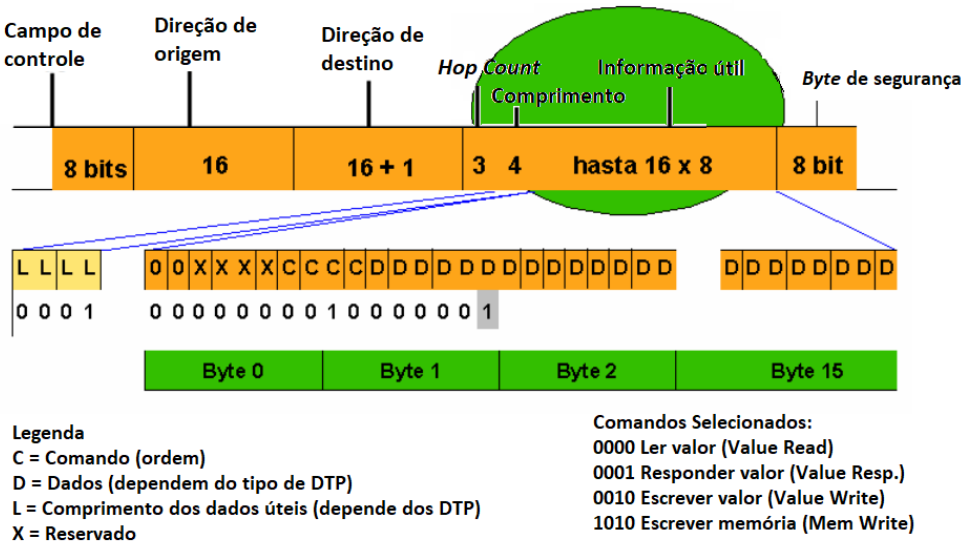


Figura 32: *DTP* 1.001, para acender /apagar.

5.2. Transmissão dos *bits* em *TP*1

Nas comunicações digitais a informação mínima que podemos ter é o bit, com os seus dois estados: zero e um. Para conseguirmos estes dois estados, no barramento *KNX*, encontramos o um para uma tensão normal e o zero para uma tensão induzida por, pelo menos, um dos componentes. Se vários componentes transmitem ao mesmo tempo, irá prevalecer o estado zero que se sobrepõe ao estado um, devido ao valor da tensão. A Figura 33, exemplifica um conjunto de dados e a sua relação com a tensão no barramento *TP KNX*. Qualquer um dos estados tem a duração descrita na seção 4.2.1, ou seja, em *TP*1 104 μs [17] [21].

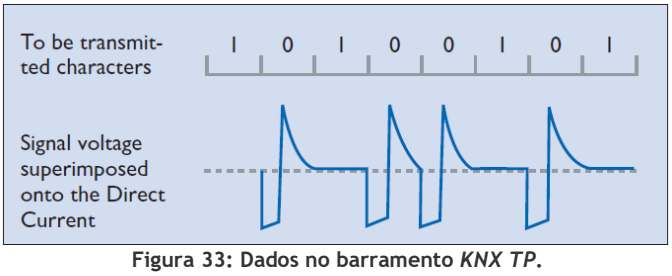


Figura 33: Dados no barramento *KNX TP*.

O acesso ao barramento é baseado no protocolo *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidance*), que salvaguarda situação de colisões entre telegramas. Quando um dispositivo pretender transmitir uma mensagem pode começar a fazê-lo imediatamente se encontrar o barramento desocupado, caso contrário, terá de aguardar até este ficar livre. Todos os dispositivos leem o barramento, enquanto transmitem, para detetarem qualquer colisão, que ocorrerá se dois dispositivos transmitirem simultaneamente uma mensagem. Como o estado

lógico zero é dominante, o dispositivo que tentar impor o estado lógico um, irá detetar o outro estado lógico. A transmissão será interrompida para que o dispositivo com a mensagem prioritária continue a faze-lo. Por fim, o dispositivo com a mensagem de prioridade mais baixa, após a outra mensagem terminar, voltará a repetir o telegrama. O protocolo *CSMA/CA* assegurasse que a rede só será ocupada por um destes dispositivos [17] [21] [22].

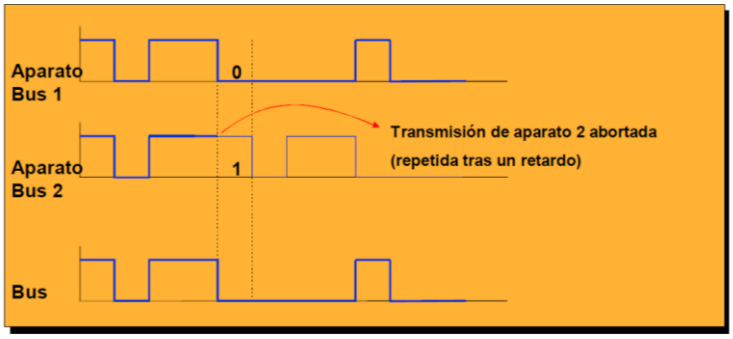


Figura 34: Exemplificação da deteção de colisões.

5.3. Transmissão simétrica em *TP*1

Os dados são transmitidos através de condutores idênticos aos da Figura 35, que são utilizados no barramento do tipo *TP*1. O protocolo *KNX*, aproveitando este par de condutores, utiliza um tipo de transmissão designado de transmissão simétrica.

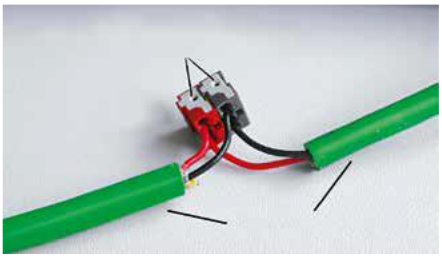


Figura 35: Cabo *TP KNX*.

Esta técnica tem a vantagem de atenuar as interferências externas pois estas, se ocorrerem, afetam da mesma forma os dois condutores e ao serem atenuadas não terão influência significativa no sinal. Na prática, uma interferência afeta os dois condutores da mesma maneira, fazendo com que esta não seja interpretada pelo recetor no barramento como uma alteração do estado lógico. É utilizada análise diferencial e se esta interferência ocorrer da mesma forma nos dois condutores não é detetada pelo componente. Na Figura 36 [21], temos o exemplo de um sinal e de uma interferência no barramento *KNX TP*. À esquerda um sinal lógico, à direita o exemplo de uma interferência [17] [21].

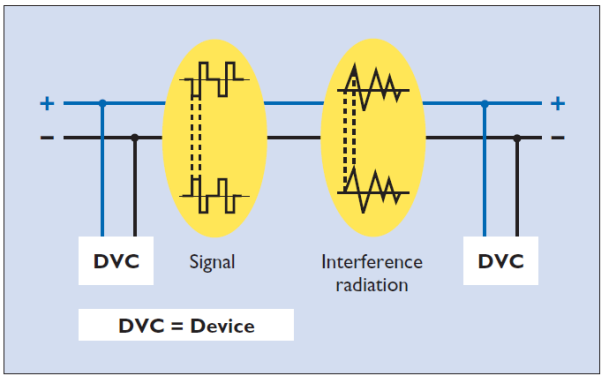


Figura 36: Transferência de dados simétrica.

A transferência simétrica ocorre porque em *KNX* não há um valor de referência em relação à Terra. Denomina-se transmissão simétrica livre de Terra. Nos dispositivos compara-se os valores da tensão entre os dois condutores. Se não há alteração temos o um lógico. Se houver uma alteração superior a 6 V temos o zero lógico que é produzido com meia onda compensada, de forma que aos 104 μs a tensão está na posição de equilíbrio [17] [19] [20] [22].

5.4. Sobreposição de dados e alimentação em *TP*1

No barramento *TP* do protocolo *KNX*, os dados transmitem-se através da alteração do valor da tensão. Esta alteração é produzida em um ou vários componentes do barramento. Nos componentes é necessário separar ou agregar os dados com a tensão de alimentação. O condensador reage com uma baixa reatância à tensão alternada, isto é, atua como um condutor e fecha o circuito no primário do transformador. Ao atuar como um transmissor, o transformador envia dados ao lado do primário, na forma de corrente alternada, que se sobrepõem à corrente continua originando o sinal lógico zero. Na Figura 37, temos o transformador primário, em cima à esquerda a negro, interligado por indução com o secundário em baixo, para onde se transferem os dados se houver corrente alternada. Ao lado do primário temos um condensador que permite estabilizar a tensão que será fornecida ao componente e desacoplar o sinal [17] [20].

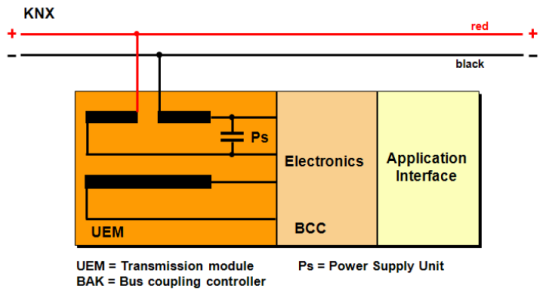


Figura 37: Circuito responsável pelo acoplamento de dados.

5.5. Ligação da fonte de alimentação ao Barramento *KNX TP*1

O cabo *TP KNX* propicia a ligação a todos os dispositivos do barramento e permite a transferência de dados pelo mesmo. Embora a tensão da fonte seja superior (30 V), a tensão dos dispositivos é de 24 V mas, na prática funcionam com tensões entre 21 V e 30 V, isto é, têm uma tolerância de funcionamento de 9 V para absorver possíveis quedas de tensão resultantes de perdas no barramento. O barramento da instalação alimenta-se através de uma bobina. Quando a tensão é continua, a bobina reage com uma baixa reatância e, por conseguinte, a frequência é de sensivelmente zero Hz. Se houver tensão alternada, passa-se exatamente o contrário e a frequência é diferente de zero. A bobina tem a função de estabilizar os dados do *barramento* alterados pelas reatâncias dos condensadores de forma a que esteja no valor de referência ao fim de um período. Na Figura 38, pode-se ver a representação da fonte de alimentação ligada ao barramento [17] [21] [22].

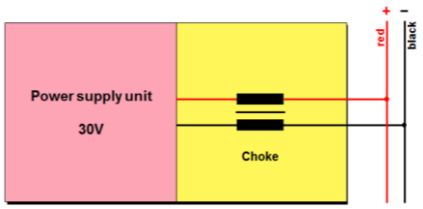


Figura 38: Fonte de alimentação *KNX* de 30 V.

Capítulo 6 - Componentes do barramento KNX. Outras caraterísticas do protocolo

6.1. Caraterísticas dos componentes físicos do protocolo *KNX*

Os componentes, do barramento *KNX*, como os *dimmers* ou sensores de presença são os componentes físicos que operacionalizam as diferentes funções de domótica numa habitação. A sua arquitetura será descrita ao longo deste capítulo. No geral são constituídos por três partes que são o acoplador do barramento (*BCU*, Bus *Coupling Unit*), o módulo da aplicação *(AM, Application Module)* e o programa de aplicação (*AP*) [17] [20] [21].

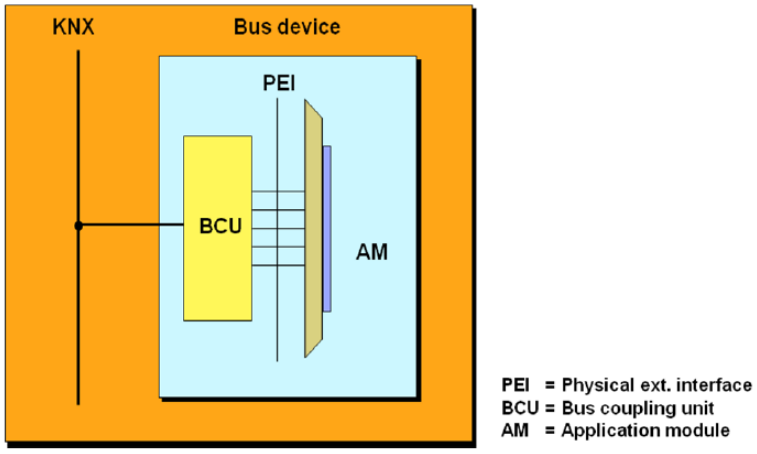


Figura 39: Arquitetura geral de um dispositivo *KNX*.

Na prática, o acoplador do barramento (*BCU*) e o módulo da Aplicação (AM) podem estar juntos ou separados, sendo sempre do mesmo fabricante. No caso de estarem separados, os componentes têm uma interface de junção padronizada, chamada de *PEI* (*Phisical External Interface*) que permite que as partes dos componentes se juntem facilmente. Estes componentes separados são, por exemplo, muito utilizados nos botões de comando, pois deixa-se a instalação pronta e no fim encaixam-se as teclas pretendidas e/ou *display*, vulgarmente designada por montagem de superfície. Tipicamente, os *PEI* de acoplamento têm 10 ou 12 pinos. No exemplo da Figura 40, temos um *PEI* com 10 pinos. Salientar que o pino seis é reservado para uma resistência padrão que permite identificar o tipo de *AM*, por exemplo 0 Ω, nada ligado, 0,50 Ω, 4 entradas binárias, e outros valores definem outras funções. Esta resistência permite verificar se o módulo AM é adequado ao programa da aplicação ou não, se não for o caso o programa de aplicação é bloqueado [17].

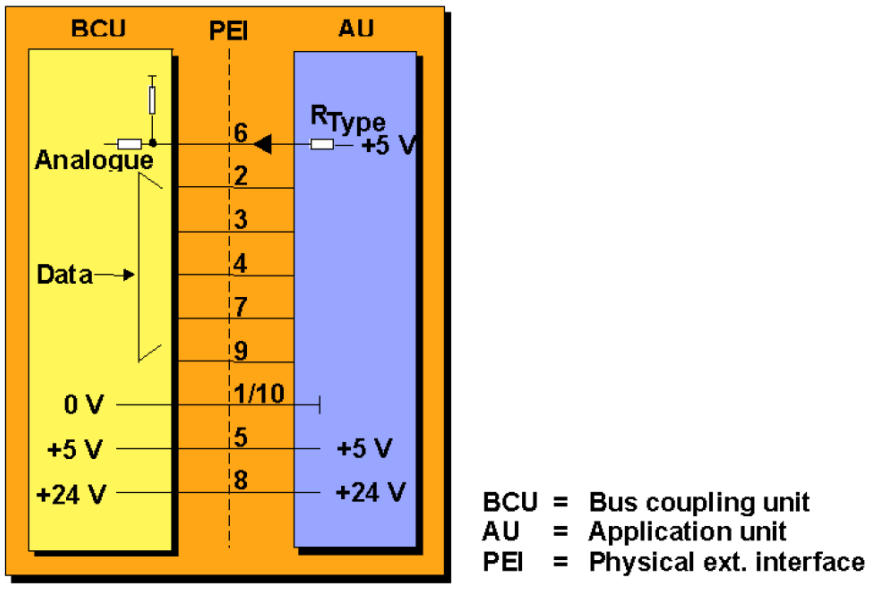


Figura 40: Exemplo de ligações PEI de 10 pinos.

O *BCU* liga-se normalmente ao barramento mediante duas fichas estandardizadas de cor negra e vermelha, respetivamente, que podem ser vistas na Figura 35. As ligações também podem ser feitas em calha *DIN*, com ligação por pressão, como se pode ver na Figura 41 [17].

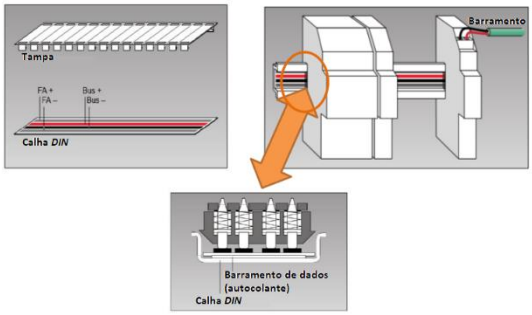


Figura 41: Barramento *KNX* em calha DIN. A ligação faz-se por perfuração através de pressão.

O *BCU* é disponibilizado montado com um módulo de Interface com o barramento, chamado *BIM* (*Bus interface module*) ou através de um circuito integrado ("*chipset*"). Fundamentalmente, um módulo *BIM* é uma *BCU* onde falta a caixa e onde são disponibilizados alguns pinos. Por outro lado, o *chipset* consiste num núcleo de um *BIM*, isto é, apenas um controlador e um módulo de transmissão (*transceiver*). Na Figura 42, podemos ver o exemplo de um *BIM* da Siemens, certificado pela *KNX* e que pode ser usada para o desenvolvimento de projetos. Para tal é necessário um programador denominado *BIM Evaluation Board*, que permite acesso completo ao microcontrolador da *BIM* [17].

Figura 42: Exemplo de um *BIM* para *KNX*, neste caso, da Siemens.

Os componentes físicos do barramento, os sensores, os atuadores ou controladores necessitam sempre de um *BCU*, uma vez que este é uma parte fundamental dos componentes *KNX*. No caso dos sensores, a unidade de aplicação envia a informação para o *BCU*, que a codifica e envia através do barramento pelo meio físico respetivo. Por outro lado, neste caso, o *BCU* verifica em intervalos regulares o estado da unidade de aplicação com o fim de detetar alterações para serem introduzidas novamente no barramento. No caso dos atuadores o processo é inverso, isto é, o *BCU* recebe a informação do barramento, descodifica e envia essa informação ao módulo de aplicação. A troca de informação entre sensores e atuadores pode ser realizada diretamente através de controladores como, por exemplo, por intermédio de controladores lógicos. Os *BCU* atualmente estão normalizados para comunicação com o meio físico par trançado, especificamente *TP*1, e Rede Elétrica *PL*110. Em *KNX* não existem acopladores para RF. Neste caso, as soluções do mercado são soluções integradas, isto é, cada fabricante desenvolve o seu hardware capaz de transferir os telegramas *KNX* RF por radio frequência [17] [20] [21].

6.2. Estrutura interna de um acoplador de barramento (*BCU*)

O *BCU* é constituído pela parte eletrónica que é necessária para a gestão das ligações, no barramento, controlando os dados que são enviados ou recebidos através deste. Esta parte física dos componentes *KNX* é responsável por filtrar as direções físicas e de grupo, extração do telegrama destinado ao dispositivo específico, verificação de erros e envio. Em síntese, a gestão de toda a informação que circula no barramento. O *BCU* é constituído por duas partes: um controlador e um *transceiver*. Por um lado, temos o controlador que contém um microcontrolador com diferentes tipos de memória. É nestas que são armazenados os dados. Existe uma memória do tipo *ROM* ou do tipo *flash*, que contém o software do sistema o qual, em regra, não pode ser alterado. Uma memória *RAM*, volátil, que armazena os dados temporários durante o funcionamento normal do dispositivo. Memória não volátil, apagável eletricamente (*EEPROM*), onde se armazena o programa de aplicação, a direção física e a tabela de direções de grupo. Por outro lado, temos o módulo de transmissão (TM) que é responsável por separar a alimentação dos dados (acoplamento através do transformador e filtro capacitivo), proteger contra uma inversão de polaridade *RPP* Figura 43, regular uma tensão de alimentação a 24V DC, inicializar a transferência dos dados de importantes da memória *RAM* se

a tensão cai abaixo dos 18 V, reinicializar o microprocessador se a tensão cair abaixo dos 5 V, amplificar e efetuar as funções lógicas para a receção / transmissão para o barramento e vigiar a temperatura da unidade. São estas caraterísticas do *BCU* que permitem que os componentes *KNX* sejam autónomos e, por isto, este é um sistema distribuídos que não necessita nenhuma unidade central de controle como por exemplo um computador. Na Figura 43 podemos visualizar a simplificação da unidade de transmissão e módulo de controle. A existência de unidades centrais é para monitorização do estado do sistema, diagnósticos ou outras funções de carater mais técnico como por exemplo servidores *KNX* que permitem acrescentar mais funções de monitorização, atuação, entre outros com os meios existentes [17] [21].

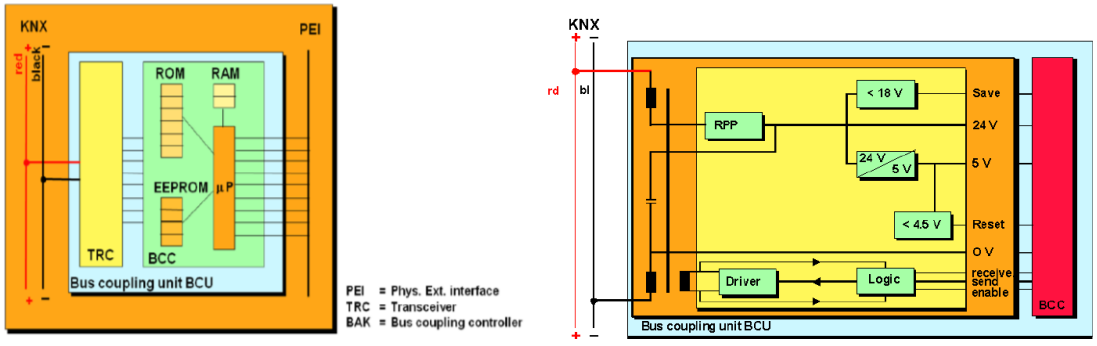


Figura 43: Partes de um *BCU*, módulo de controle e módulo de transmissão.

6.3. Considerações nos projetos *KNX*

6.3.1. A instalação. Desenho e projeto

A realização de uma instalação *KNX* requer um conjunto de fases que são as seguintes:

- Planificação prévia que deve ir de encontro ao utilizador final.

- O desenho do projeto, que ajuda a orçamentar o custo da instalação, uma vez que obriga ao estudo dos componentes necessários à instalação. Deve-se ter em conta as especificações locais e da rede de domótica. Em *KNX*, a utilização do cabo de barramento embora paralelo ao cabo de potência da rede tem que utilizar a sua própria canalização. As distâncias entre os componentes devem ser cumpridas e estar de acordo com as normas *KNX* [17] [21]:

O comprimento máximo permitido de todos os cabos é de até 1000 m;

A distância máxima entre dois aparelhos na mesma linha não pode ser superior a 700 m;

A distância máxima entre a fonte de alimentação com bobina e um aparelho não pode ser maior de 350 m.

A distância entre duas fontes de alimentação com bobina não pode ser inferior a 200 m.

- A instalação elétrica deve respeitar os regulamentos em vigor. Em Portugal as instalações elétricas são certificadas pela Certiel.

- A programação é a etapa final do projeto. Processa-se, principalmente, a partir de um computador ligado à instalação cuja ligação pode ser feita de várias maneiras. Atualmente por cabo *USB* ou pela rede *Ethernet*. No programa configuram-se os endereços físicos, os endereços de grupos e parametrizam-se os sensores e atuadores. Também se realiza a programação das tabelas de filtros nos acopladores de linha e de área.

6.4. Programar dispositivos *KNX*. O *ETS*

A principal maneira de se programarem os dispositivos de uma instalação é mediante software fornecido pela Associação *KNX*. Por norma utilizasse o *ETS*, no entanto, em janeiro 2017, para facilitar o processo, foi lançada uma nova forma de programar as instalações *KNX* de pequena e média dimensão. Uma nova aplicação denominada "*ETS Inside*", cuja interface fica disponível a partir de qualquer dispositivo móvel Windows, Apple ou Android. A licença adquire-se, na forma de *Dongle USB*, tal como a do *ETS*, mas é consideravelmente mais barata que a licença *ETS Profissional*, embora em ambos os casos seja possível programar o mesmo número dispositivos (na prática até 3000 dispositivos). Na hora da aquisição as caraterísticas e diferenças devem ser tidas em conta. Salientando apenas uma delas, uma licença "*ETS Inside*" só pode ser usada para um projeto, uma vez que é parte fixa da instalação, enquanto uma licença *ETS* pode ser usada para múltiplos projetos. Na Tabela 7, são apresentadas algumas das diferenças entre o "*ETS Inside*" e o *ETS Profissional*.

Tabela 7: *ETS Profissional* e *ETS Inside*.

	ETS Professional	*ETS Inside*
KNX meios físicos	*TP*, *PL*, *IP*, RF	*TP*, *PL*, *IP*, RF
KNX secure	Sim	Sim
Nº de Projetos	Ilimitado	1
Dispositivos	Ilimitado	Ilimitado
Dispositivos típicos	Sim	Sim
Dispositivos *Plug-In*	Sim	Não

Na Figura 44, está esquematizado o princípio de funcionamento do "*ETS Inside*". É necessário um dispositivo com uma aplicação de servidor que é disponibilizada pela Associação *KNX*. Após configurado o servidor com o "*ETS Inside*", pode-se aceder remotamente a partir de dispositivos móveis, onde deverá ser instalada a aplicação, gratuita, denominada também "*ETS Inside*" [24].

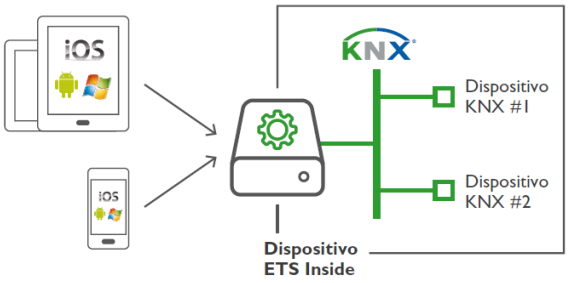


Figura 44: Princípio de instalação do *ETS Inside*.

O projeto criado no "*ETS Inside*", pode ser sincronizado com o *ETS Profissional* em qualquer altura. Relativamente ao *ETS* existem várias licenças, algumas das quais já foram mencionadas anteriormente. A versão da Licença *ETS* gratuita, permite programar até cinco dipositivos *KNX*, a versão da Licença *ETS Lite* permite programar até vinte dispositivos e, por fim, a versão da Licença *ETS Profissional* permite programar um número ilimitado de dispositivos *KNX*. Obviamente os preços diferem significativamente da versão *ETS Lite* para a *ETS Profissional*. Existe ainda uma versão Educacional que inclui uma licença *ETS Profissional* mais dez licenças *ETS Lite*. Neste caso o preço é um pouco superior à versão Profissional. Na Figura 45, pode-se ver uma visão geral do programa *ETS*.

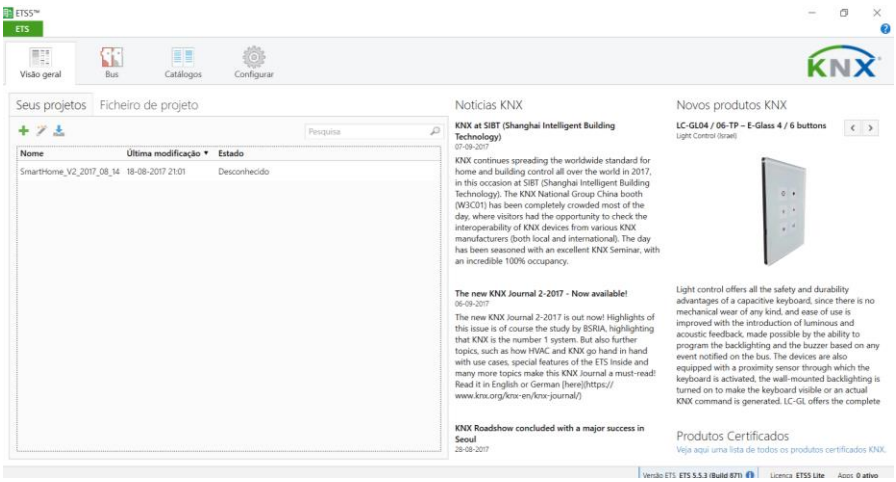


Figura 45: Visão geral do software *ETS* disponibilizado pela Associação *KNX*.

Atualmente o *ETS* corre na Versão 5. No arranque do programa *ETS*, encontramos, na parte superior quatro separadores que são: Visão Geral, BUS (barramento), Catálogos e Configurar. Na parte inferior direita, podemos verificar a versão do *ETS*, ativar ou verificar o tipo de licença e adicionar APPS. Relativamente aos separadores superiores, temos:

Visão Geral: permite criar um projeto novo, abrir um existente e exportar ou importar um projeto. Podemos ainda verificar algumas das novidades do mundo *KNX*.

BUS: permite configurar o tipo de ligação do *ETS* à instalação.

Catálogos: Separador reservado à importação dos catálogos dos produtos utilizados no projeto. Estes podem ser importados a partir do projeto depois de aberto.

Configurar: permite configurar o *ETS*, por exemplo, alterar o idioma.

Capítulo 7 - *KNX sobre a rede IP*

7.1. O protocolo *KNXnet/IP*

As redes *KNX* estão cada vez mais integradas na rede *IP*. Na Figura 46 podemos ver um exemplo de uma infraestrutura representada, à esquerda, com *TP* e à direita, com a utilização de *KNXnet/IP* routers, que são dispositivos que permitem interligar a rede *KNX* e a rede *IP*. Desta forma, a *backbone* passa a ser a rede *IP* e os acopladores de área e/ou linha deixam de ser necessários, dependendo da configuração. Na Figura 46 a *backbone* em *TP* é substituída por *IP*.

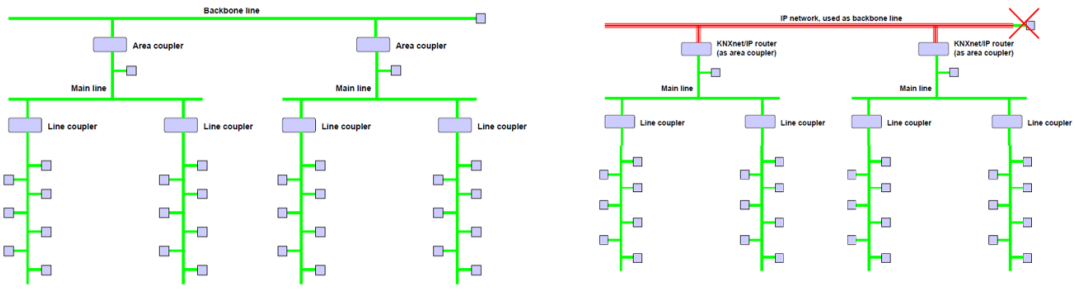


Figura 46: À esquerda a *backbone* utiliza cabo entrelaçado, à direita utiliza o cabo *Ethernet*.

Esta ligação é feita à custa do protocolo *KNXnet/IP*. A associação *KNX* herdou o EIB.net que atualizou para o protocolo *KNXnet/IP* e, como já foi referido, permite a utilização de uma rede *KNX* sobre uma rede *IP*. A utilização da *backbone* com a rede *IP* tem várias vantagens. Desde logo, permite o acesso remoto aos sensores e atuadores. A elevada velocidade deste meio faz com que não existam atrasos nas transmissões, uma vez que a velocidade de transmissão é muito superior à transmissão, por exemplo, em *TP*1. Por outro lado, o acesso remoto permite para além da monitorização e configuração dos dispositivos, o diagnóstico à distância a partir de qualquer parte do mundo, evitando deslocações desnecessárias. O protocolo *KNXnet/IP* pode ser estudado em termos do modelo de camadas semelhante ao modelo *TCP/IP* já mencionado no Capítulo 2. Contém no topo a camada de serviços *KNXnet/IP* correspondente à camada de aplicação no modelo *TCP/IP*. As restantes camadas do *KNXnet/IP*, as camadas de transporte, rede e camada física. Na Figura 47 pode-se ver a implementação de um dispositivo que implementa o protocolo *KNXnet/IP*, em termos de modelo de camadas. Como se verá, a comunicação é realizada através do protocolo *UDP*, e não *TCP*, e, por este motivo, o modelo de camadas é apresentado em função do modelo *UDP* para o protocolo *KNXnet/IP* [21] [25].

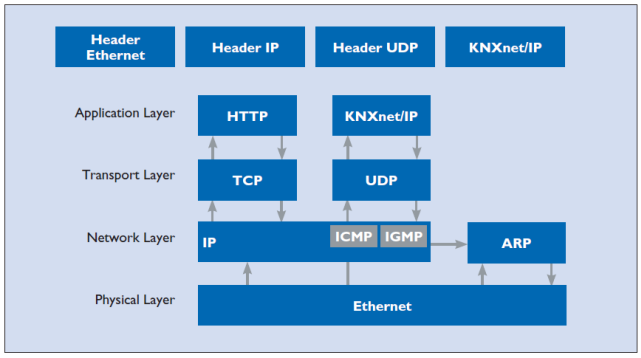


Figura 47: Modelo de camadas para um dispositivo *KNXnet/IP*.

Uma rede com o protocolo *KNXnet/IP* terá de conter no mínimo, uma sub-rede *KNX*, qualquer que seja o tipo de meio utilizado, um dispositivo que faça interface entre uma rede *KNX* e uma rede *IP* como por exemplo um *KNXnet/IP* router. Por fim, poderá ser utilizado software que permita a ligação da rede *IP* à rede *KNX*. Na Figura 48 vemos o caso mais simples de um sistema *KNXnet/IP* [26].

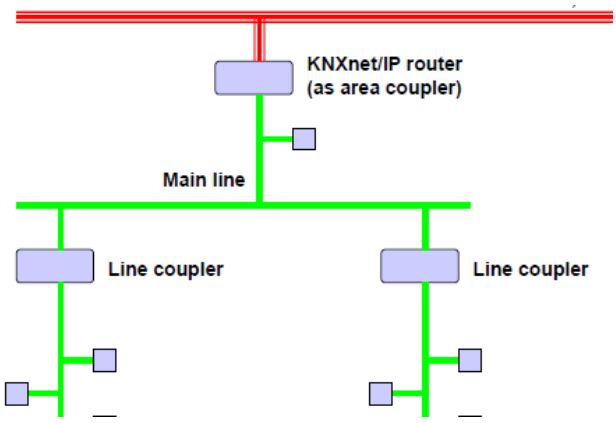


Figura 48: Rede *KNX* ligada à rede *IP*.

O protocolo *KNXnet/IP* está dividido em quatro módulos, o que permite ao programador /Engenheiro de produtos *KNXnet/IP* implementar os mais convenientes e necessários. Os módulos são os seguintes, núcleo (core), gestão de dispositivos (management), *tunnelling* e o *routing*. O núcleo é um módulo sempre presente em todas as implementações pois contém as especificações dos telegramas *KNXnet/IP*, os serviços básicos de funcionamento e uma descrição do protocolo de rede *IP*. O módulo da gestão de dispositivos define serviços para efetuar configurações e gestão de servidores *KNXnet/IP*. O módulo de *tunneling* consiste na criação de um túnel *IP*, entre um cliente *KNXnet/IP* e um *Gateway KNXnet/IP* (conexão de ponto a ponto) permitindo o envio de telegramas *KNX* para a rede *IP* e vice-versa. É um método utilizado normalmente para gestão das redes *KNX*. Foi o método utilizado no trabalho prático, abordado mais à frente para configurar a rede *KNX* a partir do programa de gestão *ETS* [21] [26].

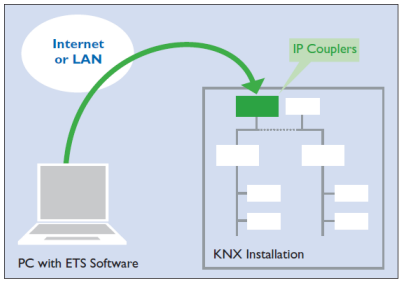


Figura 49: Ligação ponto a ponto, *tunneling*.

O módulo de *routing* é o método que permite o encaminhamento de telegramas pela rede *IP*. É normalmente utilizado para que diferentes redes *KNX* troquem telegramas (tipicamente em *multicast*ing) a partir de uma rede *IP*, mas também permite a troca de telegramas com o exterior. Os routers *KNXnet/IP* podem trocar mensagens entre si. No trabalho prático também foi implementado um *router KNXnet/IP* como método alternativo para comunicação com o *ETS* [21] [25] [26].

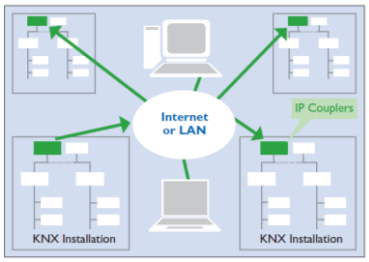


Figura 50: Ligação da *KNX* sobre *IP*.

Implementados os métodos, a comunicação utiliza o protocolo *UDP*. A comunicação em *UDP* é mais simples e rápida que a *TCP* pois é um protocolo simples e sem conexão, descrito na *RFC* 768. Ele tem a vantagem de fornecer uma entrega de dados de baixa sobrecarga. Os segmentos de comunicação em *UDP* são chamados datagramas. Na Figura 51 [27] podemos verificar a diferença entre os cabeçalhos *TCP* e *UDP* [26] [27].

Figura 51: Cabeçalho *TCP* e *UDP*.

De salientar que a comunicação alternativa seria a comunicação *unicast*, isto é, ponto a ponto. É uma solução implementada, por exemplo, entre um gestor de dispositivos (*ETS* por exemplo) e um dispositivo *KNX* específico. Não é a solução comum pelos motivos apresentados, maior simplicidade dos telegramas, mas também porque as comunicações *unicast* generalizadas levantariam problemas de engenharia complexos, difíceis de resolver. Obrigaria a desenvolver um sistema capaz de permitir ligações ponto a ponto entre os vários dispositivos, por conseguinte, a um aumento considerável do custo dos produtos *KNX*. A associação *KNX*, em particular o grupo responsável pelas comunicações *KNX* sobre *IP* considerou que as comunicações *multicast* são adequadas e mantêm os padrões de qualidade e simplicidade impostos ao protocolo *KNX*, sendo o método comum de comunicação em *IP* para o protocolo *KNX*. Relativamente à comunicação para a rede *IP* em *UDP*/*IP*, é feito o encapsulamento da camada de aplicação, isto é, dos telegramas *KNXnet*/*IP*. Estes telegramas podem conter os telegramas *KNX*, provenientes da camada física. A introdução do telegrama *KNX*, no telegrama *KNXnet*/*IP* depende dos serviços definidos pelo protocolo *KNXnet*/*IP*. Caso o módulo de gestão de dispositivos, de *tunniling* ou de *routering*, o definam são introduzidos estes telegramas na rede *IP*. A resposta a um pedido destes não tem encapsulado um telegrama *KNX*.

7.1.1. Telegramas *KNXnet/IP*

Os telegramas *KNXnet*/*IP* contêm os seguintes campos no cabeçalho:

Comprimento do cabeçalho: contém o comprimento que é fixo. Este campo pode ser alterado uma vez que está em aberto para versões futuras. Esta informação serve para identificar o começo do telegrama.

Versão do protocolo: contém e indica a versão do protocolo *KNXnet*/*IP* que é utilizada na comunicação.

Identificador do tipo de serviço *KNXnet*/*IP*: indica a ação a ser desencadeada. Contém o tipo de serviço.

Comprimento total: indica o comprimento total do telegrama.

Corpo *KNXnet*/*IP*: contém a informação útil, por exemplo um telegrama *KNX*.

A Figura 52 [21] mostra o cabeçalho simplificado de um telegrama do protocolo *KNXnet*/*IP*.

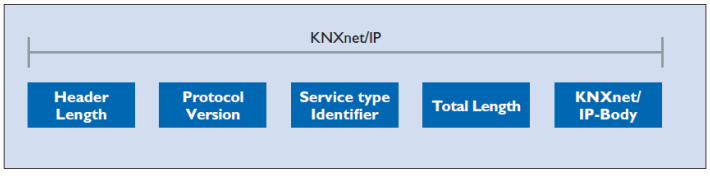


Figura 52: Estrutura simplificada do cabeçalho *KNXnet/IP*.

7.1.2. Dispositivos de comunicação *KNX* sobre *IP*

As soluções mais comuns, para a ligação da infraestrutura *KNX* à rede *IP*, são o *KNXnet/IP* router e o *Gateway KNX IP*, com caraterísticas diferentes. A primeira solução o que faz é desencapsular os telegramas *KNXnet/IP* para que possam ser introduzidos na rede *KNX* ou vice-versa. A segunda solução permite a comunicação remota, ponto a ponto, entre este e o gestor da rede *KNX*. Estes, por outro lado, utilizando telegramas específicos proprietários, para comunicarem com a infraestrutura *KNX*. Permitem, por exemplo, a construção de uma interface em que o utilizador final comunica com os componentes *KNX* utilizando uma página *Web*. Esta solução não é uma solução padronizada, isto é, não é comum a todos os fabricantes. Ambas as soluções para serem utilizadas requerem que o programador conheça a infraestrutura *KNX* e domine o protocolo *KNX*. Um *IP Gateway KNX* foi uma das soluções escolhidas e implementada no trabalho prático que será abordado mais à frente. A Figura 53 exemplifica os dipositivos físicos disponíveis que permitem a comunicação *KNX* sobre *IP*.

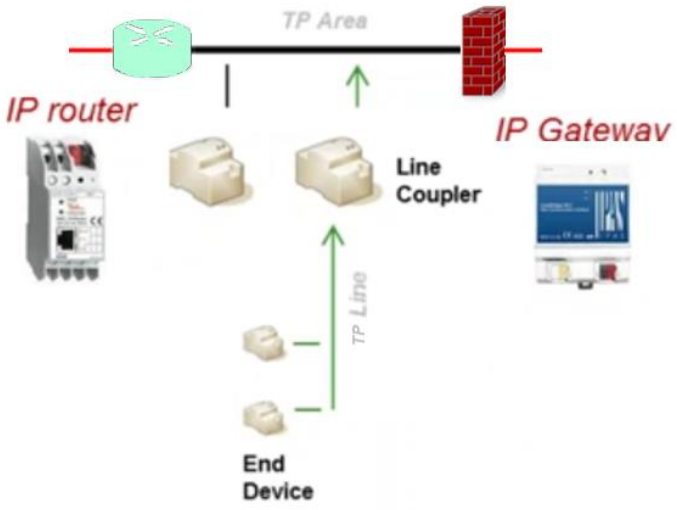


Figura 53: Dispositivos que permitem a comunicação *KNX* sobre *IP*. O *KNXnet/IP* router e o *KNX IP Gateway*.

7.1.3. Endereços individuais *KNX* de routers *KNXnet/IP* ou outros dispositivos *KNX IP*

Como referido anteriormente, numa instalação *KNX*, podemos ter o *backbone* totalmente em *IP* e ainda dispositivos *KNX IP*, isto é, um dispositivo *KNX* que utilizam o protocolo *IP* como o único meio *KNX*, Figura 54 [26]. Estes dispositivos têm para além de um *IP* um endereço individual *KNX*.

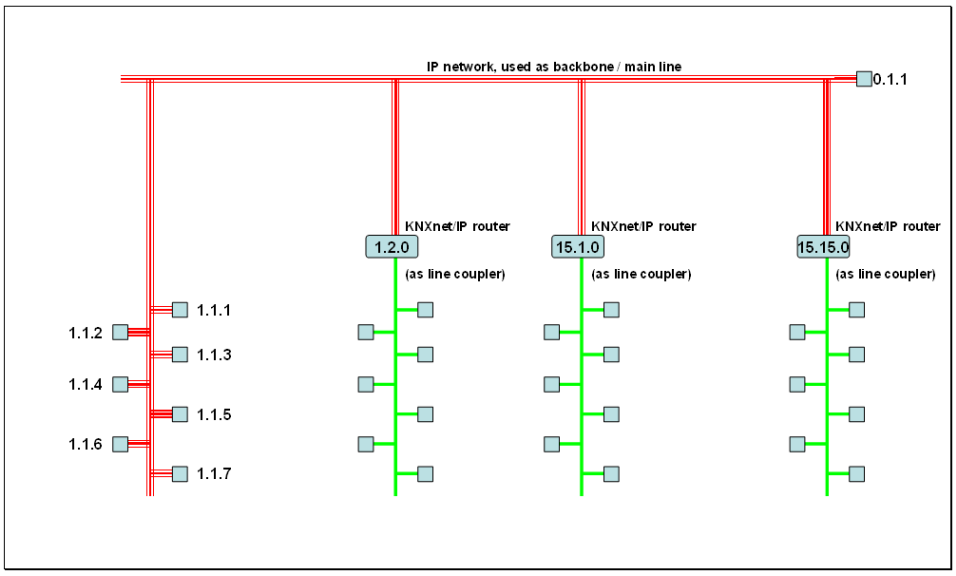


Figura 54: Exemplo de dispositivos *KNX* ligados a rede *IP*. Têm um endereço individual *KNX*.

Esta alteração, no *backbone*, leva a que seja necessário algum cuidado na atribuição destes endereços individuais aos dispositivos da rede *KNX*. As regras para atribuição de endereços *KNX* são as seguintes [26]:

Regra 1: em geral, um router *KNX*net / *IP* pode ser usado como um acoplador de linha ou um acoplador de *backbone*. O Endereço Individual possui o formato x.y.0, com x = 1 a 15 e y = 0 a 15.

Regra 2: se um *router KNXnet/IP* for aplicado como um acoplador de área com o endereço individual x.0.0 então nenhum outro *router KNXnet/IP* com o endereço individual de acoplador de linha x.y.0 (y = 1 a 15) deve ser colocado hierarquicamente abaixo deste *router KNXnet/IP*.

Regra 3: se um *router KNXnet/IP* for aplicado como um acoplador de linha (por exemplo, com o endereço individual 1.2.0), nenhum outro *router KNXnet/IP* deve ser usado com um endereço individual do acoplador de área superior (por exemplo, 1.0.0) nesta instalação.

Regra 4: se um dispositivo *IP KNX* for atribuído a uma sub-rede como um dispositivo simples (por exemplo, com endereço individual 1.0.1), esta sub-rede e qualquer sub-rede mais alta na estrutura do sistema devem conter somente dispositivos *IP KNX*.

7.1.4. Potenciais problemas do *KNX* sobre a *IP* e soluções

Nas infraestruturas *KNX* que utilizam *IP* na sua *backbone*, devido aos vários *KNXnet/IP* router podem surgir problemas. Estes problemas podem surgir em diferentes partes da infraestrutura.

A Figura 55 [26] mostra estas diferentes partes, onde podem existir problemas, na transferência de telegramas *KNX* que serão explicados a seguir.

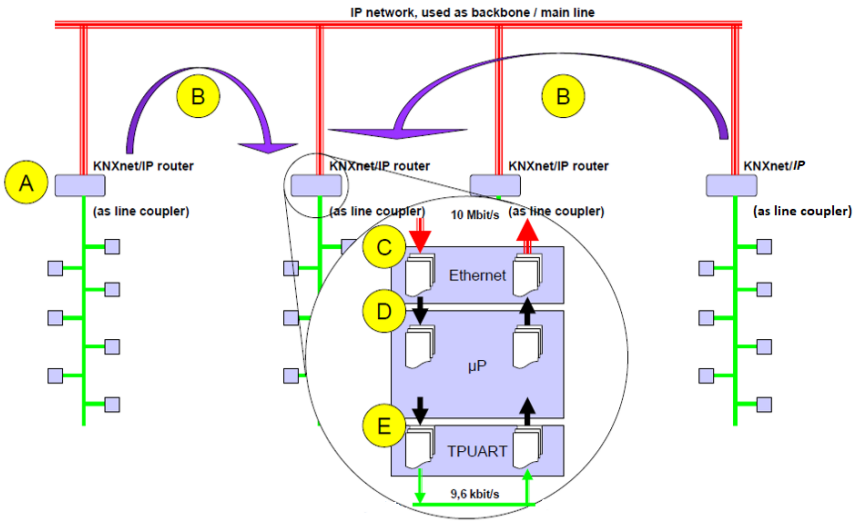


Figura 55: Sinalização de diferentes zonas de potencias problemas de *KNX* sobre *IP*.

O problema começa logo nos *KNXnet/IP* router (A) uma vez que, a transmissão de telegramas em *IP* é em *multicast* (*UDP*) e pressupõe que não há aviso de recessão, pelo que, a troca de dados não é reconhecida podendo levar à perda de telegramas. Por outro lado, a transmissão de dados em *IP* (B) é pelo menos 1000 vezes superior à transmissão de dados em outros meios *KNX*. Este facto pode fazer com que haja um estrangulamento nos *KNXnet/IP* routers (C) quando transmitem da rede *IP* para a rede *KNX* pois, pode haver perda de dados no microprocessador (D) por haver excesso de dados e este não ser capaz de os processar. A rede *KNX* só é capaz de receber até 50 telegramas por segundo em função do tipo de meio que deve ser o número máximo de telegramas que a *TPUART* ou *transceiver* (E) deve enviar para a rede *KNX*. Para uma garantia de comunicação como por exemplo a verificação do estado de um equipamento ou a ligação de um dispositivo de gestão, como o *ETS*, com os dispositivos da infraestrutura, a solução é uma solução *unicast*, isto é, ligação ponto-a-ponto. Para salvaguardar a transferência de dados os fabricantes são os responsáveis pelos requisitos dos equipamentos *KNX IP* ou *KNXnet/IP* router, isto é, estes devem ser capazes de lidar com um trafego adequado e os fabricantes são responsáveis por selecionar e projetar hardware, *firmware*, sistema operativo e /ou software aplicativo adequados. Finalmente, as informações contidas nos cabeçalhos *KNXnet/IP*, nomeadamente no campo Routing_Busy asseguram que a taxa de transferência da rede *IP* para a rede *KNX* é feita de forma a que não haja estrangulamento de dados. Estas caraterísticas asseguram uma excelente fiabilidade aos telegramas *KNX* em *IP* [26].

Capítulo 8 - Domótica habitacional, *IoT* e o protocolo *KNX*

8.1. *KNX* como parte da *IoT*

De acordo com as ideias apresentadas no Capítulo 2, relativas à *IoT*, neste capitulo será feita a relação com a domótica residencial, em particular, com o protocolo *KNX, por ser o protocolo estudado*.

Pode-se dizer que este protocolo já é uma solução da *IoT* ou, pelo menos, parte dela. A infraestrutura *KNX* utiliza um conjunto de sensores e atuadores ligados, que podem comunicar recolher e trocar informação, entre si e o mundo físico. Todos os componentes têm um número de série e dentro da rede têm um endereço físico podendo ser ligados à internet. A infraestrutura *KNX* pode utilizar vários meios de comunicação, como o par trançado (cabo), rádio frequência, *PowerLine* e *IP* como *backbone* que utilizam *KNX*/*IP* Routers para a comunicação entre diferentes partes *KNX*. A comunicação por *IP* remota também é possível através da utilização de *IP Tunneling*. Assim de acordo com o conceito de *IoT* e com as caraterísticas do protocolo *KNX*, os dispositivos *KNX* podem ser integrados na *IoT* [28].

8.2. Evolução dos dispositivos de comunicação *KNX* sobre *IP*

A utilização remota das redes tipicamente é feita com a ligação a um *KNXnet*/*IP* router ou a um *Gateway KNX* e, como vimos obriga ao conhecimento protocolo e da rede *KNX*. Este facto tem-se revelado uma desvantagem para os técnicos de TI não conhecedores de *KNX* uma vez que não existe uma solução padronizada para estes potenciais clientes. Com estas soluções, o protocolo *KNX* é de difícil integração em servidores ou aplicações *Web*. Em 2014, um dos vários Grupos de trabalho da associação *KNX*, designado de *KEB* (*KNX Executive Board*) decidiram a criação de metas chamadas "*KNX* 2020", no âmbito de acesso à rede de Internet, com o objetivo de captarem e alargarem a novos utilizadores, principalmente na área das TI, nomeadamente programadores para o desenvolvimento de novas aplicações assim como, permitir a fácil integração de instalações *KNX* em aplicações de servidores convencionais e não específicos *KNX*, como acontecia até aqui. O projeto principal ficou conhecido como *KNX Evolution Project*, que visou o desenvolvimento de novos padrões para a evolução da Estrutura *KNX*. Neste caso, definiu-se a agregação ao *Gateway* com *Serviço Web*, *Gateway WS* (*WS* do inglês *Web Service*). No fundo, uma solução que permite a integração do sistema domótico *KNX* com a Internet, isto é, a comunicação, entre diferentes aplicações *Web* e a infraestrutura física de domótica na Internet. Os Serviços *Web* são componentes de software adicional que permitem às aplicações

enviar e receber dados. Assim cada aplicação pode utilizar a sua própria linguagem de programação, mas a ponte com a rede *KNX* deverá ser uma linguagem universal, um formato intermediário. Esta nova abordagem, atualmente em expansão, permite alargar as potencialidades tanto a programadores *Web* como aos fabricantes que assim podem lançar novos produtos com estas caraterísticas [28].

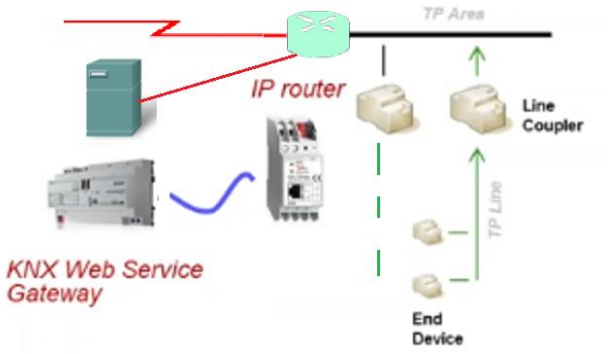


Figura 56: Serviço *Web* com ligação à rede *KNX*.

8.3. Serviços *Web (Web Service) KNX*

Resumidamente, os serviços *Web* (*WS*) são componentes de software modulares independentes que podem ser descritos, publicados e ativados através da *web*. É um software projetado para apoiar as comunicações entre máquinas, realizadas através da rede. Normalmente são implementados por aplicações e não por pessoas. Assim, uma comunicação simples e multifacetada entre serviços e sistemas *web* da automação de edifícios é possível [29]. A partir de um *Gateway* com estes *WS KNX* pode-se ler, gerar ou modificar a informação de uma instalação *KNX*. As *Gateways WS KNX* utilizam *RESTful Web Services*. É uma solução técnica que permite o acesso à rede *KNX* utilizando o acesso a recursos e aos recursos *KNX*, isto é, permitem o acesso à infraestrutura de forma mais fácil a partir de uma biblioteca. A informação é sempre importada, para o *Gateway WS KNX*, numa forma standard a partir do *ETS* pelo responsável técnico da instalação que efetua a programação dos componentes do sistema. No entanto deixa de ser necessário à utilização de telegramas *KNXnet/IP* ou proprietários para a comunicação entre o *WS* e a rede *KNX*. A utilização deste novo componente físico permite que a implementação das aplicações possa ser utilizada por um cliente *Web*, sem que seja utilizado e conhecido o protocolo *KNX*. Dos modelos conhecidos dissidiu-se por três que são *OBIX, OPC UA* ou *BACnet / WS*. Qualquer um dos métodos pode ser utilizado, embora tendencialmente por estratégia de mercado e razões comerciais a *KNX* incentiva a utilização do *OBIX*. Os métodos *BACnet / WS* e *OBIX* foram desenvolvidos e preparados para a automação de edifícios e estão disponíveis gratuitamente para o público em geral. OBIX é de particular interesse devido ao seu modelo de dados extensível, isto é, dá a possibilidade de definir qualquer tipo de objeto que seja utilizado para descrever tipos de dados (classes) e operações (assinaturas do método) [28].

8.4. *OBIX* baseado em *KNX WS*

O *OBIX* (*open building information exchange*) é uma forma de etiquetar de forma estandardizada os diferentes componentes *KNX*. É uma iniciativa ao nível da indústria para definir mecanismos baseados em serviços XML e *Web* para o desenvolvimento de sistemas de controle padronizados. Utiliza "*Querys*" (perguntas), muito utilizado em clientes baseados em *RESTful* e que pode ser utilizado também para na domótica residencial. Com a utilização de um *Web Service*, diferentes dispositivos podem comunicar entre si através da mesma base de dados, sem nenhum deles interferir com a informação armazenada diretamente, mas apenas através dos métodos disponíveis de forma automática. A comunicação do *Web Service* com o cliente é feita via protocolo *HTTP* ou *HTTPS* para maior segurança. Os dados são enviados na linguagem *XML*, e comparados numa biblioteca específica chamada *Calimero* [30].

8.4.1. Biblioteca *Calimero*

Calimero, é uma biblioteca de *APIs Java*, isto é, regras pré-definidas, que formam a base para aplicações *KNX*/EIB. Foi desenvolvido por estudantes da *University of Technology* em *Viena de Áustria* e da *University of Applied Sciences* em *Deggendorf* e apresentado na *KNX Scientific Conference,* 2005. Permite que aplicações desenvolvidas possam ter a capacidade de acesso e controlo, a uma instalação *KNX*, local ou remotamente. Esta biblioteca padroniza a forma de acesso à base de dados *KNX*, não sendo necessário um conhecimento detalhado do protocolo nem da instalação *KNX*. Simplifica muito a forma de acesso ao barramento *KNX* pois no seu funcionamento, a biblioteca *Calimero*, estabelece uma ligação, tanto de leitura como escrita, com o dispositivo *KNXnet/IP* e atua como um gestor de eventos entre este e a aplicação *web*. A ligação entre a biblioteca *Calimero* e a instalação é feita no modo *tunneling*. Todos os eventos ficam registados em base de dados [30] [31].

8.5. Domótica habitacional e *IoT*. Uma realidade presente

As áreas de aplicação do protocolo *KNX* cobrem praticamente todas as necessidades residenciais, existindo dispositivos de diferentes fabricantes que cobrem estas mesmas necessidades. A Figura 57 [32] mostra as diferentes áreas de atuação do protocolo *KNX*.

Figura 57: Diferentes campos de atuação, na domótica, do protocolo *KNX*.

A partir do momento que se ligam os diferentes dispositivos à Internet torna-se mais fácil usar dados para funções automatizadas, para apresentar valores e estados de uma instalação *KNX* e avaliá-los. Sistemas autónomos podem atuar em situações concretas, por exemplo adequar a temperatura de uma habitação, adequar a luminosidade e muitas outras aplicações. Juntamente com outros sensores pode-se otimizar a gestão de energia. Mais ainda, pode-se fazer uma gestão de recursos. Num complexo residencial, por exemplo, podem-se utilizar sensores comuns para diferentes residências. O exemplo mais simples seria a utilização de uma estação meteorológica comum em vez de múltiplas. Através do *KNX IoT* a Automação de Edifícios passa a ter um enorme novo potencial. Esta nova troca aberta de dados entre os sistemas de TI e os sistemas de automação de edifícios possibilita a utilização de aplicativos melhorados com elevados e múltiplos benefícios [29]. Esta ligação começa a ficar mais facilitada tendo em conta este novo *Gateway KNX WS* que consegue mapear de forma mais fácil o Projeto *KNX*. A nova solução *KNX-IoT* consiste na utilização deste *Gateway WS* para ligar a rede *KNX* à internet. De um lado aplicativos, gestão técnica do edifício, smartphones e outros, comunicam através de serviços *web* com o *Gateway*. Assim, a aplicação dum cliente *web* é capaz de pesquisar dados no *Gateway* dos serviços *web*, com telegramas de texto unificados e transferi-los. Do outro lado encontra-se o habitual protocolo *KNX*. No entanto, para que possam ser reconhecidos os parâmetros do Sistema *KNX* do lado da infraestrutura *IP*, o projeto *ETS* tem que ser exportado para o *Gateway* dos serviços *web KNX* (*KNX WS Gateway*). Para este fim foi disponibilizada uma nova aplicação de exportação do *ETS* (*ETS Exporter App*) [29]. A diferença substancial relativamente aos métodos clássicos mencionados anteriormente é que o protocolo passa a utilizar um método padronizado para o desenvolvimento de novas aplicações. Na segunda parte do trabalho prático valida-se a utilização de um *Gateway WS KNX* associada à maquete miniaturizada de uma habitação que foi construída para implementar algumas das áreas de atuação *KNX* possíveis. A Figura 58 resume a implementação de um *WS* [30] [33].

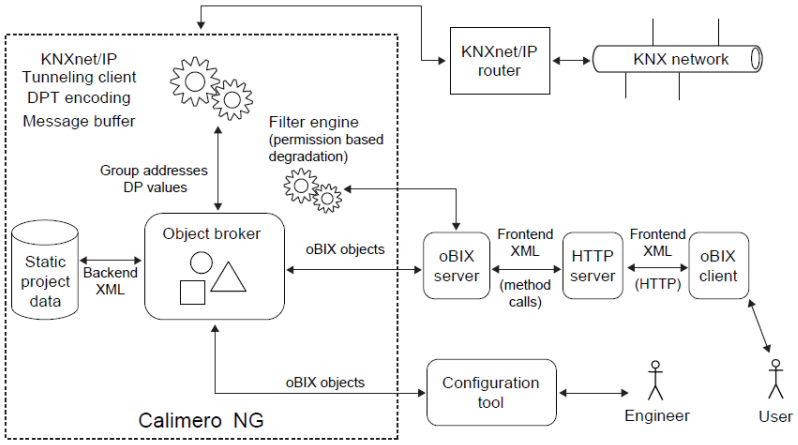


Figura 58: Resumo de implementação de um servidor (*Gateway KNX WS*) com *OBIX*.

Capítulo 9 - Validação Prática: exemplos de aplicações

9.1. Introdução

Para além da parte teórica planificou-se e desenvolveu-se uma validação prática utilizando o protocolo *KNX* com o objetivo de ligar os componentes deste à Internet. Para o caso de estudo construi-se uma maqueta, na qual foram instalados alguns dos componentes característicos de uma habitação (iluminação, tomadas e motorização). A escolha recaiu nos componentes mais comuns para uma maior simplificação da estrutura. O princípio de funcionamento é idêntico para outros tipos de componentes. Esta maqueta foi desenvolvida para que, em situações futuras, permita adicionar e estudar novos dispositivos *KNX*. A Figura 59 mostra o resultado final relativo à parte de iluminação e tomadas.

Figura 59: Aspeto da maqueta construída para a validação do trabalho teórico.

A Figura 60 mostra o resultado final da maqueta com a motorização de uma porta / portada. Qualquer outro tipo de motorização terá uma implementação e funcionamento semelhantes.

Figura 60: Aspeto final parte da maqueta relativa à motorização.

9.2. Planificação e etapas de execução

Para ir de encontro aos objetivos da validação prática, a construção e ligação à internet de um sistema domótico planificou-se a infraestrutura domótica. No essencial consiste na instalação constituída pelos sensores e atuadores para a automatização da infraestrutura.

9.2.1. Projeto

Para a ligação à internet utiliza-se um *Gateway KNX router* e um *Gateway WS KNX IP*, este último exterior à infraestrutura, mas ligado a um *KNXnet/IP router* que está incluído na infraestrutura. A estrutura foi projetada para ter duas partes alimentadas separadamente. Uma parte com todos os componentes *KNX* que fica ligada a uma *UPS* (*uninterruptible power supply*) e restante à rede elétrica diretamente. O objetivo é o de uma proteção acrescida dos componentes *KNX* e evitar atrasos no arranque, em caso de falta de energia. A Figura 61 mostra o aspeto parcial do quadro elétrico da maqueta e a identificação dos dois circuitos.

Figura 61: Quadro elétrico da maqueta.

Por fim foi estruturada para simular diferentes divisões de uma habitação real, neste caso *Hall* de entrada, sala e um quarto.

9.2.2. Identificação das partes

Numa infraestrutura são necessários sensores e atuadores. Por outro lado, os componentes de ligação à rede *IP* e à *Internet*. A lista de componentes utilizados foi a seguinte:

- Fonte de Alimentação *KNX* 640 mA, utilizada para a alimentação dos componentes *KNX*.

- Fonte de alimentação auxiliar, utilizada para alimentar o *Gateway KNX*.

- Atuador 8 canais, utilizado para ligar/desligar iluminação, tomadas entre outros ou pode ser configurado para *shutter*, utilizando dois dos canais. Com esta configuração foi utilizado para trabalhar com a motorização.

- *Dimmer* 4 canais, utilizada para a regulação da luz numa das partes da maqueta. Por opção, neste projeto, só foi utilizado um dos canais.

- Entradas binárias (4 canais), utilizadas para comando com alguns dos interrutores.

- Entradas binárias 8 (canais), utilizadas para o comando com os restantes interrutores.

- Sensor de presença, utilizado para a deteção de pessoas.

- Gateway KNX IP proprietário (*IPAS Home Control HCC*) utilizada para a execução de uma *interface web* para o acesso e controle remoto.

- *Router KNXnet/IP*, utilizado para a configuração do *Gateway KNX IP* e para ligação ao *Gateway WS KNX*.

- Servidor *web* ou *Gateway WS KNX IP*, utilizado para implementar o *Web Service* (dispositivo externo à maqueta).

A Figura 62 mostra alguns dos componentes *KNX* utilizados.

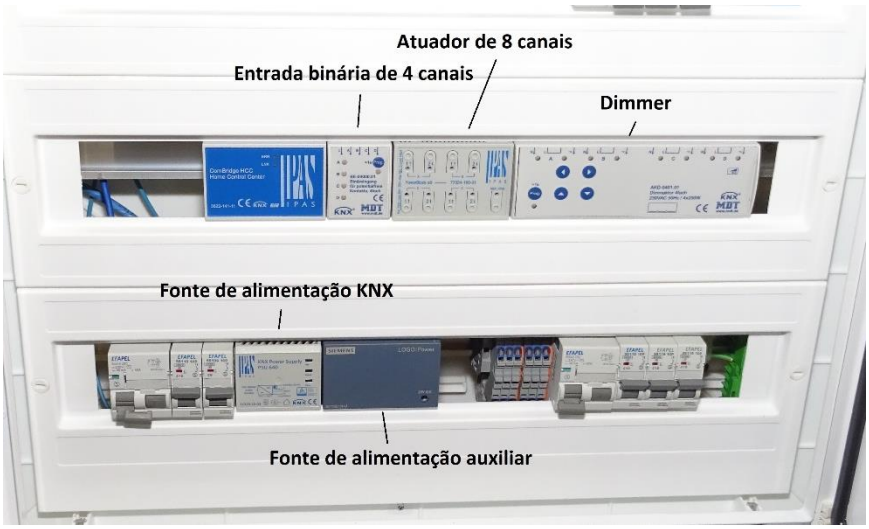


Figura 62: Alguns dos componentes KNX utilizados.

9.2.3. Programação com o *ETS*

Implementada a maqueta foi necessário proceder à programação dos componentes e para o feito utilizou-se o *"S-mode" (System Mode)* com recurso ao software *ETS*. É sempre necessário criar os endereços individuais e dos endereços de grupo. No *ETS utiliza-se* o separador "Visão Geral", para criar um novo projeto. Em primeiro lugar cria-se a topologia do edifício, neste caso um piso único com o *Hall* de entrada, uma sala e um quarto. Em seguida procede-se à importação das bibliotecas para cada componente utilizado. Estas bibliotecas são fornecidas pelos fabricantes dos componentes e contêm todas as funcionalidades dos mesmos.

Seguidamente criam-se os objetos de grupo. Por fim ligam-se os diferentes componentes nesses mesmos objetos de grupo, para se definirem as funções a executar na maqueta e/ou num edifício real. É necessário configurar todos os parâmetros dos componentes, por exemplo o *dimmer* pôde ser configurado para ter um valor mínimo e máximo de luminosidade. O último passo consiste em descarregar todas as configurações para os componentes. Na maquete puderam-se efetuar os testes. A Figura 63 mostra o aspeto do *ETS* após descarga com sucesso das configurações para os componentes. Salientar que a primeira vez que cada endereço individual é configurado o programa informa que se deve carregar no botão de programação que existe em cada componente.

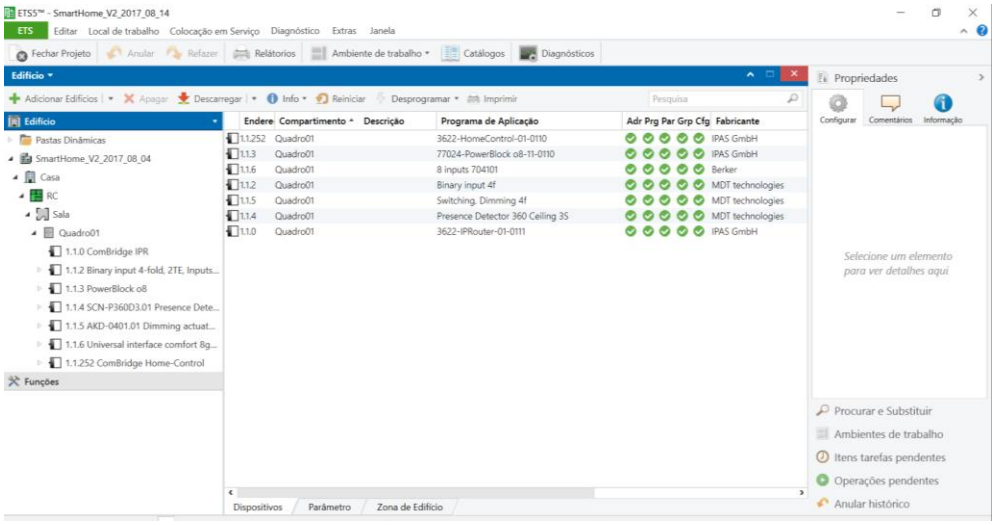


Figura 63: Aspeto do *ETS* após descarregadas todas as configurações dos componentes.

9.3. Ligação à Internet

Para a ligação do sistema domótico à internet implementaram-se os dois dispositivos possíveis e existentes atualmente. Utilizou-se um *Gateway KNX IP* e implementou-se um *Gateway WS KNX* com recurso a um servidor *web* externo à maqueta.

9.3.1. Dispositivo proprietário, o *Gateway KNX IP*

Após analisadas algumas das soluções do mercado escolheu-se o produto *HCC* da *IPAS* uma vez que tem uma excelente relação qualidade preço. Permite a fixação em calha *DIN* e contém um servidor *web*. Suporta a ligação de até 250 objetos *KNX* e utilização até 1000 endereços de grupo. Permite criar duas interfaces distintas, uma projetada livremente com um editor da *Web* e, outra, uma visualização gráfica otimizada como um aplicativo da *Web* para smartphones ou *tablets*. Este dispositivo também oferece extensas funções lógicas, horários de programação, cenas, alarmes e funções de e-mail. Foi desenvolvido especificamente para utilizadores e integradores de sistemas de pequenos e médios edifícios. Permite que seja controlado a qualquer momento e de qualquer lugar do mundo. A Figura 64 mostra o aspeto deste dispositivo.

Figura 64: *Gateway KNX IP*.

Para a configuração deste dispositivo específico é necessário proceder a exportação da estrutura da infraestrutura a partir do *ETS*. No separador "Visão Geral", deve-se exportar em "Exportar OPC" a partir da opção "Extras", Figura 65.

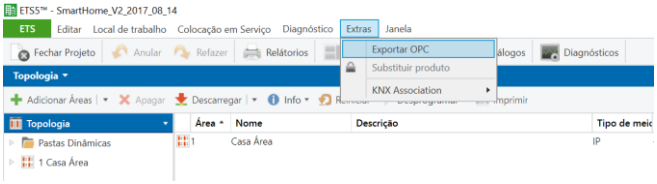


Figura 65: Na opção "Extras", selecionar "Exportar OPC".

Este procedimento gera um ficheiro com uma extensão *esf*. Este mesmo ficheiro deve ser importado a partir do editor disponibilizado no *Gateway*, Figura 66. Este ficheiro contém todos os *DTP* e endereços de grupo criados no *ETS*.

Figura 66: Aspeto do editor *web*. Importação do ficheiro do *ETS* com as configurações da infraestrutura.

A construção da página *web*, com as indicações do fabricante, foi adequada à maqueta. A Figura 67mostra o aspeto final da página *web*.

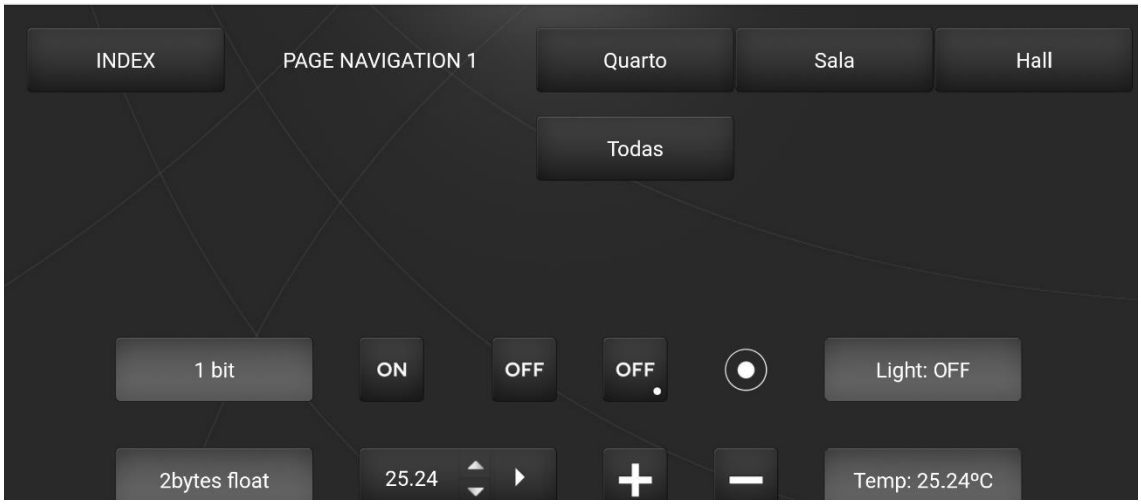


Figura 67: Página *web* para acesso remoto à infraestrutura.

A segunda opção de programação, a visualização gráfica otimizada, foi bastante mais fácil de implementar uma vez que o modelo está pré-definido. A Figura 68 mostra o aspeto desta página *web*.

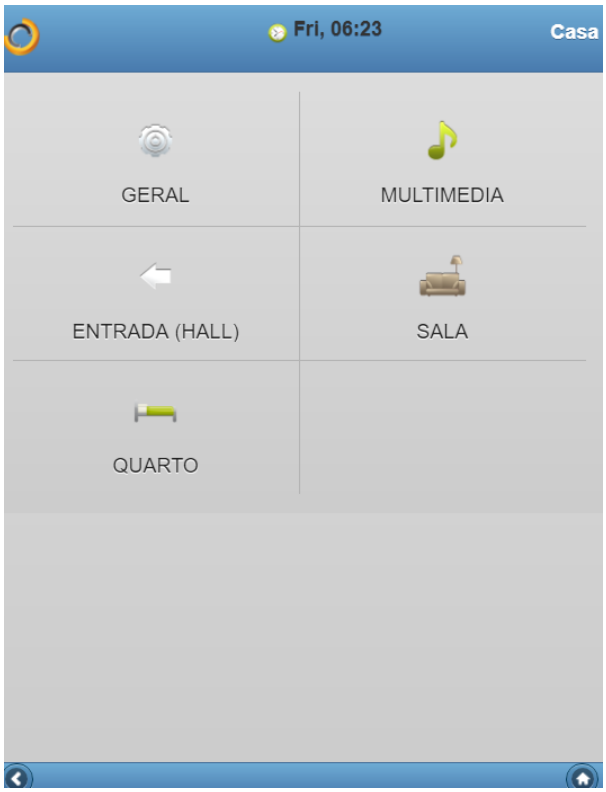


Figura 68: Página *web* otimizada para smartphones e tablets.

O último passo, para um acesso remoto à infraestrutura, foi o da configuração da porta de acesso remoto por *IP*. Esta teve de ser alterada uma vez que o servidor *web* utilizado tinha a

mesma porta de acesso. Para facilitar um acesso remoto configurou-se um *DDNS* (*Dynamic Domain Name System)*, isto é um sistema que permite utilizar o mesmo *DNS* (*Domain Name System)* para um *IP* dinâmico. Este processo funcionou sem problemas. Salientar apenas que o fabricante não permite utilizar ligações remotas seguras em *HTTPS*. A solução poderia ser a da implementação de uma ligação privada ou *VPN* (*Virtual private network*).

9.3.2. *OBIX* como *Web Service*, o *Web Sevice KNX IP*

A segunda solução consistiu em implementar um *Gateway WS KNX IP*. Para o efeito foi utilizado um servidor *web* onde foi implementado o serviço *OBIX*. Utilizou-se um servidor virtual, onde foi implementado uma imagem disponibilizada pela associação *KNX* para testes. O servidor utilizado foi um *Qnap TS 470* que permite, numa das suas aplicações chamada "*Container Station"*, criar máquinas virtuais. Nesta aplicação descarregou-se uma imagem, a partir de outra plataforma *web* chamada *Docker*, com o nome *KNXGateway*-1. Este processo foi implementado desta forma, porque o servidor mencionado já se encontrava disponível para testes e a alternativa seria a aquisição de um dispositivo físico para o mesmo efeito. A associação *KNX* menciona o *Raspberry Pi*. Instalada a imagem procederam-se aos testes. A Figura 69 mostra a aplicação do servidor "*Container Station"* utilizada com a imagem do *Gateway WS KNX IP* já importada.

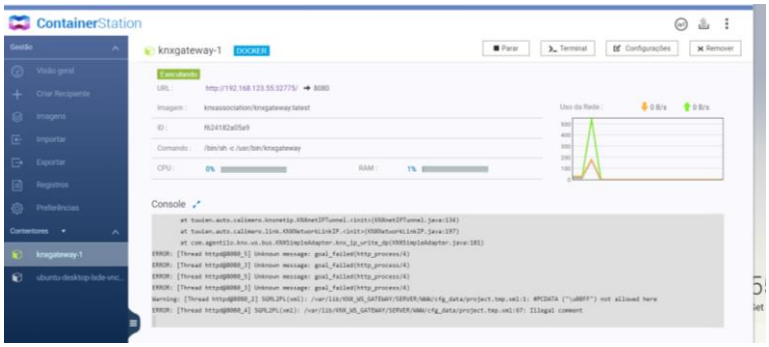


Figura 69: Aplicação para máquinas virtuais.

Num computador, a partir de um browser acede-se a virtualização do *Gateway KNX WS*. A Figura 70 mostra a página *web* que permite aceder a este *WS* [31].

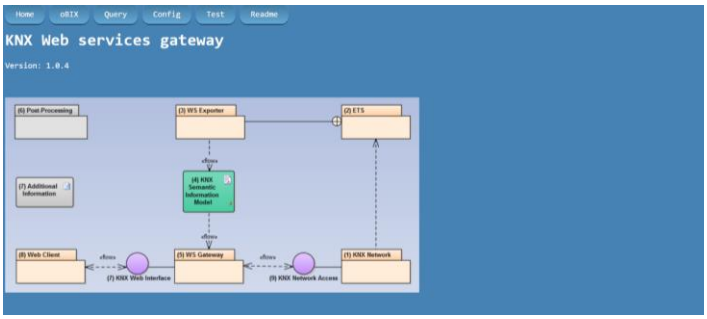


Figura 70: WS disponibilizado para testes pela associação KNX.

Para se testar o *WS* é necessário importar um ficheiro *XML* com os dados da instalação *KNX*. Este ficheiro deve ser primeiro exportado a partir do *ETS*. Neste programa no separador "Extras" deve-se proceder a exportação em "*Web service exporter*", Figura 71. Salientar que esta aplicação "*Web service exporter*" deve ser instalada no *ETS* a partir da *Web* e é disponibilizada gratuitamente pela associação *KNX*.

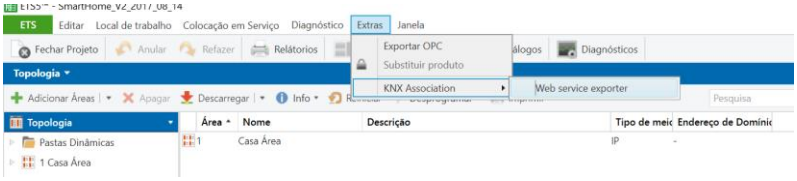


Figura 71: É necessário proceder a exportação para um ficheiro *XML*, a partir do *ETS*, com as configurações da instalação.

É necessário configurar a máquina de testes, o *Gateway KNX WS*. Esta máquina deve-se ligar ao *KNXnet/IP router* da instalação. Na opção *"Config"*, Figura 72, deve-se alterar o *IP* para o atual do router e deve-se carregar o ficheiro *XML*. Feitos estes procedimentos, a máquina pode ser testada [30] [31].

Figura 72: Opção *"Config"* do *WS*.

No *Gateway KNX WS* com *OBIX* ficam disponíveis todos os dispositivos da infraestrutura KNX. Podem-se por exemplo obter os estados lógicos das portas dos atuadores e alterar as mesmas.

Na maqueta pode-se constatar uma alteração ou mudança de estado nos atuadores. A Figura 73 mostra os dispositivos disponíveis na infraestrutura KNX.

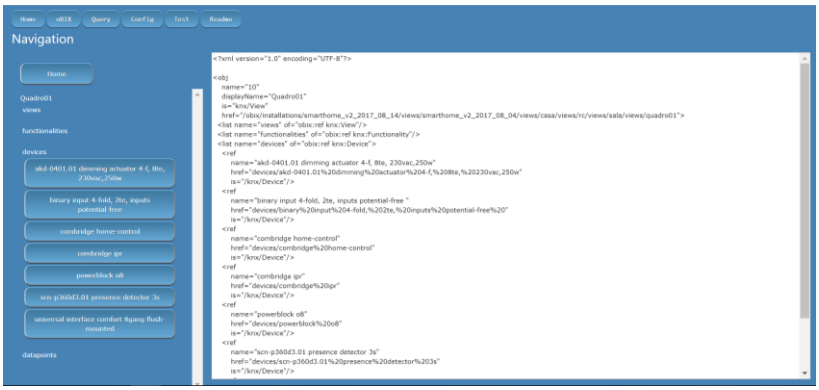


Figura 73: Os dispositivos da infraestrutura KNX são exibidos à esquerda.

No sepador "*Test*" podem-se fazer testes com os *DTP* e os endereços de grupo do protocolo *KNX*. Foi necessário fazer testes para a validação e tal como no dispositivo anterior utilizou-se o mesmo *DDNS* (*Dynamic Domain Name System)*. Como foi utiliza a virtualização disponibilizada a página *web* ficou estanque e não foram possíveis alterações. No entanto este processo também funcionou sem problemas e sem dúvida acarreta um potencial enorme para técnicos TI que podem desenvolver as suas aplicações sem a necessidade de conhecimento em *KNX* [31].

Capítulo 10 - *IoT* e a domótica. A *SmartHome*

10.1. Cenários futuros de domótica

A área tecnológica evolui de tal ordem que se torna difícil traçar um cenário no longo prazo. A domótica com os avanços tecnológicos passará a ter dispositivos cada vez mais poderosos de reconhecimento de voz, reconhecimento facial e um conjunto de reconhecimento biométrico poderoso. Os sensores existem em número cada vez maior e em áreas mais abrangentes e a área residencial não é exceção. A ligação entre estes sensores e dispositivos permitirá que na área residencial surjam cada vez mais soluções e uma maior autonomia nas tarefas domésticas. Este conceito leva-nos ao conceito de Casa Inteligente. O objetivo da Casa Inteligente é o de proporcionar uma qualidade de vida melhor aumentando o conforto, segurança e mais serviços. Os especialistas acreditam que, no futuro, a casa inteligente será gerida por inteligência artificial onde no limite tudo é controlado por máquinas. A ideia de casa inteligente é que os habitantes possam utilizar gestos e voz para controlar os atuadores residenciais. A casa deve ser capaz de reconhecer os seus moradores, a sua posição para que adeque a infraestrutura à pessoa [34]. Na prática, muitos destes cenários já são realidade. Com a IoT todos os dispositivos tenderão a estar na mesma rede pelo que surge um aumento de possibilidades sem precedentes.

A nível do protocolo *KNX* já estão traçadas as metas que permitirão a evolução do protocolo para os próximos anos, no âmbito do projeto *KNX* 2020. O *IP* por exemplo, passará a ser nativo para todos os dispositivos com a introdução de maior proteção no protocolo KNXnet/IP para este meio. Isto permitirá a padronização de funcionalidades o que permitirá o desenvolvimento de novas aplicações *web* e tornará a ligação entre dispositivos muito mais facilitada. Esta será uma área com um forte crescimento. É uma estratégia para o alargamento do mercado no âmbito deste protocolo e simultaneamente uma fácil integração, dos componentes *KNX*, na *IoT*. A figura mostra o esquema de dispositivos *KNX* para ligação nativa *IP* e com configurações automáticas incluídas para uma maior simplificação das tarefas de desenvolvimento de uma infraestrutura *KNX*. A Figura 74 esquematiza dispositivos *KNX* com *IP* nativo e a sua ligação à *IoT* [35].

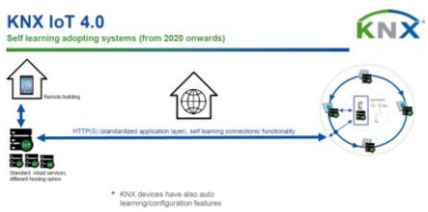


Figura 74: Evolução do protocolo *KNX*, com o *IP* a ser o meio de comunicação nativo.

Capítulo 11 - Conclusão e crítica

Esta dissertação teve como objetivo principal estudar a integração dos componentes de domótica residencial na *IoT*.

Para se alcançar este objetivo estudou-se pormenorizadamente o protocolo *KNX* uma vez que é o mais utilizado na Europa. De vários protocolos analisados verificou-se que o protocolo *KNX* tem, hoje em dia no mercado mundial, mais de 400 fabricantes em 33 países que fabricam produtos, que cobrem as principais áreas de atuação de domótica incluindo as que têm maior aplicabilidade como é o caso da segurança, motorizações, eficiência energética e conforto. Por outro lado, é um protocolo distribuído o que o torna menos vulnerável a falhas em relação a outros protocolos. Em termos de barramento de comunicação é bastante abrangente e permite a utilização de diferentes meios de comunicação, entre os quais a rede *IP* sobre *Ethernet*. É precisamente este meio que permite a ligação de uma infraestrutura *KNX* à *Internet*. Para tal verifica-se a existência de dois tipos de dispositivos que são o *Gateway KNX* e o *Gateway WS KNX IP*. A primeira solução implementa soluções proprietárias que são distintas de fabricante para fabricante. A segunda solução permite implementar uma solução padronizada de troca de dados, com recurso a uma biblioteca, entre a infraestrutura *KNX* e um cliente *web*. Utiliza uma solução do tipo *RESTful* para troca de informação entre as duas redes.

Para validação destes dois tipos de dispositivos a infraestrutura domótica (maqueta) contruída de raiz, acabou por ser uma mais valia. Permitiu conhecer o protocolo *KNX* em mais pormenor. Da investigação feita, soluções implementa-las e alterações finais resultou uma bancada de trabalho que permitirá, se necessário, estudar e testar mais facilmente novos dispositivos.

Das duas aplicações *web* utilizadas nos testes dos dispositivos mencionados. A página *web* alojada no *Gateway KNX* proprietária revelou-se bastante abrangente. Aponta-se como desvantagem o facto de ser fechada. A segunda, ligada a um *Web Service*, e com um potencial teórico bastante superior acabou apenas por permitir verificar o estado lógico dos componentes e fazer pequenos testes. Embora fora do âmbito deste trabalho teria sido interessante desenvolver uma aplicação *web* para comunicar com este Gateway *Web Service KNX*. Tal não foi possível por limitação do tempo.

Através da utilização do *Web Service KNX* passamos a ter à disposição um conjunto de dados e uma nova forma de ligarmos a infraestrutura *KNX* a um cliente *Web* de forma padronizada sem que seja necessário o conhecimento do protocolo *KNX*. Esta estratégia permite o alargamento da domótica habitacional aos técnicos de TI.

O *ETS* é uma ferramenta de trabalho fundamental que é necessária para a configuração da infraestrutura domótica e para a exportação, no final, de dados para a programação das aplicações *web* a serem desenvolvidas.

Ambas as soluções funcionam remotamente sem problemas, embora também fora do âmbito deste trabalho, teria sido uma mais valia implementar diferentes soluções com recurso a politicas de segurança, por exemplo a criação de uma *VPN* (*Virtual private network*) entre outras.

A introdução de novas aplicações com a utilização destes sensores e atuadores ligados à Internet leva-nos à *IoT*. Temos cada vez mais máquinas conectadas entre si a acederem a dados dos sensores e dos dispositivos eletrónicos em quantidades e proporções incalculáveis. A "*Internet* das Coisas" instala-se como uma grande inovação nas nossas vidas e, ao mesmo tempo, praticamente invisível aos nossos olhos.

Por fim, salientar que a nível pessoal e profissional pretendo desenvolver mais trabalhos nesta área principalmente em projetos que envolvam o desenvolvimento de plataformas *Web*, para o acesso remoto a instalações *KNX*. Também aprofundar o estudo do protocolo *KNX Secure*, que ficou de fora no âmbito deste trabalho, mas é fundamental na proteção de instalações KNX.

Capítulo 12 - Bibliografia

[1] E. Cavalcante, M. P. Alves, T. Batista, F. C. Delicato e P. F. Pires, “An Analysis of Reference Architectures for the Internet of Things,” em *CobRA '15 Proceedings of the 1st International Workshop on Exploring Component-based Techniques for Constructing Reference Architectures*, Montréal, 2015.

[2] G. L. Jamil, C. R. M. Pessoa, P. H. d. S. Santos e T. Geremias, *Análise de discurso em estudos de múltiplos casos sobre a implementação do Protocolo IPv6 nas Organizações.*, São Paulo, SP: USP, 2015.

[3] T. B. d. Silva, M. Rosa, C. R. M. Pessoa e . G. L. Jamil, “A INTERNET DAS COISAS: SERÁ A INTERNET DO FUTURO OU ESTÁ PRESTES A SE TORNAR A REALIDADE DO PRESENTE?,” 22 01 2015. [Online]. Available: http://www.fumec.br/revistas/eol/article/view/2961.

[4] C. Segura e H. R. Hildebrand, *Políticas de Mercado e a Indústria de Entretenimento Audiovisual*, São Carlos: I Jornada Internacional GEMInIS, 2014.

[5] D. Evans, Cisco Internet Business Solutions Group, 2011.

[6] J. Bradley, J. Barbier e D. Handler, “Embracing the Internet of Everything: To Capture Your Share of $14.4 Trillion (Cisco),” 2013. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.. [Acedido em 01 04 2017].

[7] J. L. Morais e J. M. G. Pereira, Guia Técnico das Instalações Elétricas, CERTIL, 2007.

[8] GreenLeaf, Realizador, *Webinar DomoLeaf - Niveau 1*. [Filme]. França: GreenLeaf, 2016.

[9] V. Junior, “Protocolos,” Junior, Valdeci, 26 09 2015. [Online]. Available: http://1430831522039-valdeci-junior.blogspot.pt/2015/09/protocolos-protocolos-de-internet-e-um.html. [Acedido em 16 11 2016].

[10] B. P. Santos, L. A. M. Silva, C. S. F. S. Celes, J. B. B. Neto, B. S. Peres, M. A. M. Vieira, L. F. M. Vieira, O. p. Goussevskaia e A. A. F. Loureiro, “Internet das Coisas: da Teoria à Prática,” 3 julho 2016. [Online]. Available: http://www.sbrc2016.ufba.br/downloads/anais/MinicursosSBRC2016.pdf. [Acedido em 03 08 2017].

[11] P. Fletcher, “Current IoT Security Threat Landscape,” Alert Logic, 26 07 2017. [Online]. Available: http://2ndwatch.com/blog/current-iot-security-threat-landscape/. [Acedido em 28 08 2017].

[12] SISLITE, “O QUE É A DOMÓTICA?,” SISLITE, 21 10 2016. [Online]. Available: http://www.sislite.pt/domus.htm. [Acedido em 17 1 2017].

[13] EPSIG, “AUTOMATIZACIÓN INTEGRAL DE EDIFICIOS,” 2015. [Online]. Available: http://isa.uniovi.es/docencia/AutomEdificios/transparencias/Generalidades2.pdf. [Acedido em 11 02 2017].

[14] N. S.r.l., “Manuale di DOMOTICA - Un riepilogo sui requisiti richiesti ai sistemi domotici alla luce delle correnti tecnologie,” S.r.l., Novatekno, Venezia, 2005.

[15] DOMOPRAC, “Domótica Pratica paso a paso,” DomoPrac, 19 09 2016. [Online]. Available: http://www.domoprac.com/mapa-de-protocolos-domoticos.html. [Acedido em 05 05 2017].

[16] K. Association, “KNX,” KNX Association, 14 03 2017. [Online]. Available: https://www.knx.org/knx-en/index.php. [Acedido em 14 03 2017].

[17] KNX, “Home and Building Management Systems,” KNX, Bruxelas, 2014.

[18] IKNX Integraciones, “Curso Iniciacion Al KNX,” IKNX Ingeniería, [Online]. Available: http://www.iknx.es/archivos/documental/2890738d8b7e3b998b994114caa6b7a4.pdf. [Acedido em 04 08 2017].

[19] European Installation Bus Association sc (EIBA), Técnica de Proyectos en Instalaciones con EIB, Alemanha: EIBA scrl, 2000.

[20] KNX, “ Webinar: KNX System - Telegrams and Electronics,” KNX, Bruxelas, 2017.

[21] KNX, The KNX standard – the basics, Bruxelas: KNX, KNX.

[22] KNX Assotiation, KNX System Specifications, Architecture, Bruxelas: KNX Assotiation, 2009.

[23] KNX, System-architecture, Bruxelas: Konnex Association, 2004.

[24] KNX, “O novo ETS Inside,” *Notícias KNX,* vol. 1, nº O novo ETS Inside – Inteligente, Simples, Seguro, p. 6, 2016.

[25] WEINZIERL, “KNX over IP - New Solutions for KNX Installations,” WEINZIERL ENGINEERING, Burgkirchen, 2013.

[26] J. Langels, “KNX IP – using IP networks as KNX medium,” Siemens AG, Regensburg, 2010.

[27] CISCO, “CCNA Exploration 4.0 - Fundamentos de Rede,” CISCO Networking Academy, Texas, 2009.

[28] KNX, Realizador, *Webinar - KNX IoT*. [Filme]. Bruxelas: KNX, 2017.

[29] KNX, “KNX Internet das Coisas-Integração simples pelos Serviços Web KNX,” *Notícias KNX*, nº Serviços Web e Automação de Edifícios, p. 8, 2016.

[30] G. N. a. W. K. Matthias Neugschwandtner, “Web Services in Building Automation: Mapping KNX to oBIX,” IEEE, Vienna, Austria, 2007.

[31] KNX, “KNX Web services Gateway IoT-1 version 1.0.4,” KNX, Bruxelas, 2017.

[32] KNX, “KNX The worldwide STANDARD for home and building control,” KNX Association International, 01 2017. [Online]. Available: https://www.knx.org/media/docs/downloads/Marketing/Presentations/HVAC-For-Manufacturers/HVAC-For-Manufacturers_en.pdf. [Acedido em 24 02 2017].

[33] J. H. -. A. G. f. K. i. Gérôme Bovet, “Introducing the Web-of-Things in Building Automation: A Gateway for KNX installations,” em *10th international Conference on Informatics in Control*, Reykjavik, Iceland., 2013.

[34] A. M. Rodríguez e M. Á. F. Lastra, “La casa inteligente,” Universidade Carlos III de Madrid, 31 08 2009. [Online]. Available: http://www.it.uc3m.es/jvillena/irc/practicas/08-09/24.pdf. [Acedido em 05 04 2017].

[35] KNX, “KNX Internet of Things (IoT) - New perspective`s on KNXfor HVAC applications,” KNX, Bruxelas, 2017.

[36] J. B. Warlick, B. Stewart e M. &. Martin, “IEEE vTools EVENTS,” IEEE, 2016. [Online]. Available: https://meetings.vtools.ieee.org/m/39794. [Acedido em 03 08 2016].

[37] P. T. M. I. a. D. M. P. Hamernik, “Classification of Functions in Smart Home,” *International Journal of Information and Education Technology, Vol 2*, vol. 2, nº Classification of Functions in Smart Home, p. 149 a 155, 2012.

[38] P. T. M. I. a. D. M. P. Hamernik, “Classification of Functions in Smart Home,” *International Journal of Information and Education Technology*, vol. 2, nº Classification of Functions in Smart Home, p. 149 a 155, 2012.

Anexos

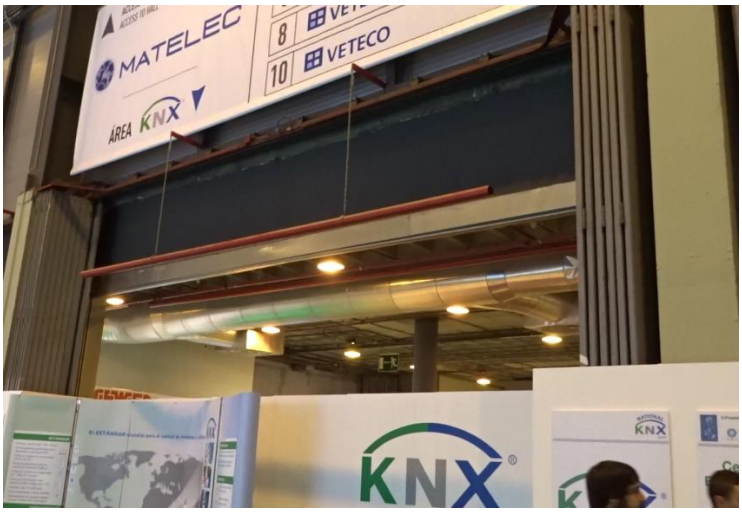
Visitas de Estudo e Certificações relacionadas com esta Dissertação

Visitas de Estudo

Para implementar esta dissertação foi importante um conjunto de Visitas de estudo que efetuei.
Visita à IFEMA, Madrid 28 outubro de 2016.

MATELEC: SALÓN INTERNACIONAL DE SOLUCIONES PARA LA INDUSTRIA ELÉCTRICA Y ELECTRÓNICA.

Novidades nas áreas da domótica e eletrónica.



Visita à Exponor, Matosinhos a 18 de fevereiro 2017.

INTERDECORAÇÃO: Casa, Hotelaria, Decoração e Brinde.

Novidades na área da iluminação.

Visita à IFEMA, Madrid a 28 de fevereiro 2017.

CLIMATIZACION: Salón Internacional de Aire Acondicionado, Calefacción, Ventilación y Refrigeración

GENERA: Feria Internacional de Energía y Medio Ambiente

Novidades no âmbito da eficiência energética.

Visita à Fil, Lisboa a 6 de maio 2017.

SEGUREX: Salão Internacional de proteção, segurança e defesa.

Novidades na deteção de intrusão, segurança e alarmes.

Certificações


KNX ETS5 eCampus

Certificate of Achievement

Pedro Pimparel

ha superado con éxito el eCampus KNX

Curso de ETS

3rd January 2017

Curso Grado: 100%

ID-Usuario: 54093

Webinars

My Training

My Courses

You don't have any courses

My Webinars

Webinar	Registration date	Status
KNX IoT	06/12/2016 16:25:44	Accepted
KNX Electrical and installation considerations	13/01/2017 20:33:41	Accepted
ETS Inside	26/01/2017 12:13:38	Accepted
KNX Principles	26/01/2017 12:14:45	Accepted
ETS Apps	26/01/2017 12:15:18	Accepted