

UNIVERSIDADE FEDERAL DE OURO PRETO
UFOP
ESCOLA DE MINAS – EM
DEPARTAMENTO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO E
TÉCNICAS FUNDAMENTAIS – DECAT

SEGURANÇA COMO COMPONENTE FUNDAMENTAL DO SISTEMA DE
AUTOMAÇÃO PREDIAL

MONOGRAFIA DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E
AUTOMAÇÃO

LUCIANA GOMES CASTANHEIRA

Ouro Preto, 2005
LUCIANA GOMES CASTANHEIRA

**SEGURANÇA COMO COMPONENTE FUNDAMENTAL DO SISTEMA DE
AUTOMAÇÃO PREDIAL**

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como parte dos requisitos para a obtenção de Grau em Engenheiro de Controle e Automação.

Orientador: André C. Silva

Co-Orientador: Luiz Fernando Rísoli Alves

Ouro Preto
Escola de Minas – UFOP

Monografia defendida e aprovada, em 25 de julho de 2005, pela comissão avaliadora constituída pelos professores:

AGRADECIMENTOS

Durante todo o desenvolvimento da trabalho tive muitas condições para a realização do mesmo.

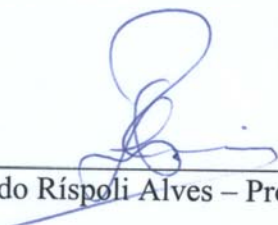
Deixo aqui meu sincero agradecimento a todas as pessoas que de alguma forma contribuíram para isso.

A essas pessoas, citadas abaixo, deixo um obrigado especial.

Aos professores do DECAT, Luiz Fernando Rísoli e Helder Arthur, ao professor do DECOM, André C. Silva, as pessoas do grupo de discussão da Aurenide e ao grupo de pessoas da PUC - RS.



André Carlos Silva – Orientador



Luiz Fernando Rísoli Alves – Professor convidado



Paulo Marcos de Barros Monteiro – Professor convidado



AGRADECIMENTOS

Durante todo o desenvolvimento do trabalho tive ajudas incondicionais para a qualidade do mesmo.

Deixo aqui meu sincero agradecimento a toas as pessoas que de alguma forma contribuíram para isso.

A essas pessoas, citadas abaixo, deixo um obrigada especial.

Aos professores do DECAT, Luiz Fernando Ríspoli e Henor Arthur, ao professor do DECOM, André C. Silva, às pessoas do grupo de discussão da Aureside e ao grupo de pessoas da PUC – RS.

SUMÁRIO

| | | |
|-------|--|----|
| 1 | INTRODUÇÃO | 1 |
| 1.1 | Histórico..... | 1 |
| 1.2 | Motivação | 4 |
| 1.3 | Estruturação do Texto | 5 |
| 1.4 | Objetivos..... | 6 |
| 2 | REVISÃO BIBLIOGRÁFICA | 7 |
| 2.1 | Integração..... | 7 |
| 2.2 | Sistema..... | 9 |
| 2.2.1 | O Enfoque Sistemico Adotado | 10 |
| 2.2.2 | Propriedade do Sistema | 11 |
| 2.2.3 | Conclusão sobre o Enfoque Sistemico Adotado para esta Investigação. | 13 |
| 2.3 | Domótica..... | 13 |
| 2.3.1 | Benefícios da Domótica..... | 16 |
| 2.4 | Segurança..... | 18 |
| 3 | ARQUITETURA DO SISTEMA | 20 |
| 4 | PROTOCOLO DE CONTROLE..... | 22 |
| 4.1 | Introdução | 22 |
| 4.2 | Características e Requisitos de Protocolos | 23 |
| 4.3 | Protocolos analisados..... | 24 |
| 5 | <i>CONTROLLER AREA NETWORK – CAN</i> | 28 |
| 5.1 | Aplicações..... | 28 |
| 5.2 | Conceitos Básicos | 28 |
| 5.2.1 | Formato dos pacotes | 29 |
| 5.2.2 | Pacote de Dados..... | 29 |
| 5.2.3 | Pacote de Requisição de Dados | 31 |

| | | |
|-------|--|----|
| 5.2.4 | Pacote de Erro..... | 32 |
| 5.2.5 | Pacote de <i>Overload</i> | 34 |
| 5.2.6 | Arbitração | 34 |
| 5.2.7 | <i>Bit-Timing</i> | 35 |
| 5.2.8 | Sincronismo | 35 |
| 5.3 | Camada Física..... | 35 |
| 6 | CONEXÕES | 37 |
| 6.1 | Tecnologia Bluetooth..... | 37 |
| 6.1.1 | Tecnologia | 37 |
| 6.1.2 | Esquema de Acesso Múltiplo | 39 |
| 6.1.3 | Controle de Acesso ao Meio..... | 40 |
| 6.1.4 | Estabelecendo Conexões..... | 40 |
| 6.1.5 | Tipos de <i>Links</i> | 41 |
| 6.2 | Tecnologia Wi-Fi..... | 42 |
| 6.2.1 | Segurança..... | 43 |
| 6.3 | Tecnologia Wi-Max..... | 44 |
| 7 | CÂMERAS DE VÍDEO | 46 |
| 7.1 | Definições | 46 |
| 7.2 | Sensores CMOS x Sensores CCD | 47 |
| 7.3 | Câmeras Estudadas | 48 |
| 7.4 | Sistema <i>GeoVision</i> | 48 |
| 7.4.1 | Características..... | 49 |
| 7.5 | Multiplexador..... | 50 |
| 7.6 | <i>Watchguard</i> | 51 |
| 7.6.1 | Aplicações..... | 52 |
| 7.7 | Monitoração Remota sem-fio via Internet ou Intranet..... | 52 |
| 7.7.1 | Benefícios: | 53 |
| 7.7.2 | Características:..... | 53 |
| 7.8 | Disponibilizando Imagens na Internet | 54 |
| 8 | RECOMENDAÇÕES | 56 |
| 9 | CONSIDERAÇÕES FINAIS | 58 |

LISTA DAS FIGURAS

| | |
|--|----|
| Figura 1.1 – Aplicações do projeto..... | 4 |
| Figura 2.1 – Integrador. | 8 |
| Figura 2.2 – Teleação..... | 15 |
| Figura 3.1 – Arquitetura do Sistema. | 20 |
| Figura 5.1 – Formato de um pacote de dados CAN..... | 29 |
| Figura 5.2 – Campo de arbitração..... | 30 |
| Figura 5.3 – Requisição remota de dados. | 32 |
| Figura 5.4 – Pacote de requisição de dados CAN..... | 32 |
| Figura 5.5 – Pacote de erro CAN..... | 33 |
| Figura 6.1 – Tipos de redes formadas entre dispositivos <i>Bluetooth</i> | 39 |
| Figura 7.1 - Exemplo da rede trabalhando com a câmera. | 54 |

LISTA DAS TABELAS

| | |
|--|----|
| Tabela 4.1 – Tabela comparativa entre protocolos | 25 |
| Tabela 4.2 – Legenda da tabela comparativa de protocolos | 26 |
| Tabela 5.1 – Comparativo entre CAN padrão e estendido | 29 |

RESUMO

Os sistemas de automação, tanto predial como residencial, têm crescido espantosamente. Hoje se depara normalmente com uma residência, até de pequeno porte, praticamente autônoma. A questão da segurança pessoal é um marco para este crescimento. O ideal para um sistema de automação é a comunicação entre os dispositivos da casa. Por exemplo, o sistema de segurança deve interagir com o sistema de *home theater* e também com o sistema de iluminação. Com isso surgiram novos conceitos como domótica (termo utilizado para designar toda residência que emprega serviços automatizados relacionados à gestão de energia, comunicação, conforto ambiental, segurança pessoal e patrimonial) e integração (qualificação de um profissional que atenda às exigências desse novo mercado possibilitando a criação, o desenvolvimento e a implantação dos sistemas domóticos). Para essa integração o primeiro passo do projeto é a escolha certa da arquitetura do sistema e seu protocolo de comunicação. Hoje já se pode desfrutar, inclusive, de comunicação sem fio – tecnologia *bluetooth* ou *wi-fi* – além das redes normais. Com o foco em segurança uma importante etapa é a escolha das câmeras de vídeo, com as características necessárias. Além disso, no projeto descreve-se como disponibilizar as imagens dessas câmeras na internet ou intranet. Finalizou-se o trabalho com algumas recomendações, onde se ressaltou o uso desse mesmo estudo para aplicações em mineração, comércio e até repartições históricas.

ABSTRACT

Automatic systems, as in buildings as in residences, have grown amazingly. Today it is come across a lot of residences, even these of small practically self governed. The question of the personal security guard is a landmark for this growth. The ideal for an automatic system is the communication among the devices of the house. For example, the security system must interact with the home theater system and with the lighting system. With this, new concepts had appeared as “*domotique*” (used term to assign all residences that use services automatized related to the energy management, communication, ambient comfort, security personal and patrimonial) and integration (qualification of a professional that takes care of to the requirements of this new market making possible the creation, the development and the implantation of the “*domotiques*” systems). For this integration, the first step of the project is the correct choice of the architecture of the system and its protocol of communication. Today, it is possible to enjoy, communication wireless - technology bluetooth or wi-fi - beyond the normal nets. With the focus in security, an important stage is the choice of the video cameras, with the necessary characteristics. Moreover, the project descripts how to dispose the images of these cameras in Internet or Intranet. The work finished with some recommendations, where the use of this technology is stood out for applications in mining, commerce and until historical distributions.

1 INTRODUÇÃO

Prédios inteligentes e sistemas domóticos têm atraído crescente interesse, por possibilitarem a atuação supervisionada e não supervisionada de dispositivos eletrônicos em uma residência, exercendo tarefas complexas e interagindo com usuários e com o meio físico. A utilização de tais dispositivos no ambiente residencial deflagra uma série de discussões e questões em várias outras disciplinas, quando o comportamento humano é avaliado. Desta forma, o desenvolvimento de residências inteligentes reúne esforços de Engenharia, Ciência da Computação, Inteligência Artificial, Psicologia, Sociologia e Filosofia, caracterizando-se como uma área multidisciplinar.

Este trabalho é um estudo de um sistema que tem a finalidade de permitir que pessoas possam administrar seus lares remotamente, de uma forma simples, com um custo baixo (implantação e administração), utilizando uma plataforma portátil e flexível a avanços tecnológicos, facilitando a implementação da domótica em lares, escritórios e prédios.

O foco principal do trabalho é na área de segurança patrimonial e pessoal.

1.1 Histórico

Segundo Neves (2002), até o final da década de 70, os computadores eram utilizados principalmente para resolver problemas de engenharia e problemas administrativos. A preocupação dos programadores concentrava-se na resolução dos

problemas, ficando a interação com o usuário em segundo plano. Esta comunicação era bastante rudimentar.

A interação com o usuário estava em segundo plano devido às limitações impostas pelos recursos computacionais da época, que eram limitados quanto à memória e aos tipos de dispositivos gráficos. Com o avanço tecnológico estas limitações foram deixando de existir e o uso dos computadores foi se difundindo para outras áreas, até alcançar o uso doméstico, com a difusão dos microcomputadores. A partir daí os computadores passaram a ser limitados não pela sua capacidade computacional, mas sim pela capacidade dos programas de se comunicarem com os usuários.

No final da década de 70, o centro de pesquisa da Xerox criou o sistema *Star* baseado na metáfora de uma mesa de trabalho (*desktop*) para fazer a interação homem-máquina. A partir daí os computadores ficaram cada vez menores, mais potentes, e principalmente, mais interativos. Com esses avanços pode-se dizer que hoje se consegue automatizar mais da metade das atividades de uma residência.

A noção de automação para prédios e residências inicialmente foi baseada na industrial, bem conhecida e difundida há mais tempo. Porém, em virtude da diferente realidade entre o uso dos dois tipos de arquiteturas, têm sido criadas tecnologias dedicadas para ambientes onde não se dispõe de espaço para grandes centrais controladoras e pesados sistemas de cabeamento. Em uma residência, no entanto, não são necessárias as complexas lógicas e dispositivos que controlam pesados processos de produção, mas em contrapartida surgem diversos tipos de interfaces, equipamentos, configurações e a necessidade de gerenciamento de tráfego como o multimídia (centenas de Mbps, em rajadas) até o tráfego de telemetria (dezenas de bps, constante).

Segundo Bolzani (2004, p. 47), o desejo de automação em projetos de pequeno e médio porte, com características comerciais ou residenciais, começou a surgir na década de 80, quando companhias como a Leviton e X10 Corp. começaram a desenvolver sistemas de automação predial. Com o grande número de aplicações e oportunidades geradas pelo computador pessoal, pelo surgimento da Internet e pelo barateamento do *hardware*, criou-se uma nova cultura de acesso à informação digitalizada. Esses fatores permitiram elevar o projeto elétrico de seu nível convencional para um nível onde todas as suas funções desenvolvidas estejam integradas e trabalhando em conjunto. Por mais

moderno que possa ser um sistema de iluminação, aquecimento ou um eletrodoméstico, se ele trabalha sem se integrar com o restante, ele é apenas mais um equipamento dentro de casa.

Algumas características fundamentais que estão presentes em um sistema inteligente, ou seja, automatizado:

- Capacidade para integrar todos os sistemas – os sistemas interligados por meio da rede doméstica devem possibilitar o monitoramento e o controle externos, bem como atualização remota de *software* e detecção de falhas.
- Atuação em condições variadas – o sistema deve ser capaz de operar em condições adversas (clima, vibrações, falta de energia) e prover múltiplas interfaces para os diferentes usuários, segundo o entendimento tecnológico, idade, etc., bem como auxiliar portadores de deficiência.
- Memória – o sistema deve ser capaz de memorizar suas funções principais mesmo em regime de falta de energia, deve possibilitar a criação de um histórico das últimas funções realizadas e prover meios de checagem e auditoria destas funções.
- Noção temporal – o sistema deve ter a noção de tempo, bem como dia e noite e estações climáticas a fim de possibilitar a execução de processos e atividades baseadas nestes aspectos.
- Fácil relação com o usuário – o sistema deve prover interfaces de fácil acesso e usabilidade, pois os usuários detêm diferentes níveis de instrução e entendimento sobre novas tecnologias.
- Facilidade de reprogramação – o sistema deve permitir a fácil reprogramação dos equipamentos e prover ajustes pré-gravados em casos de falha ou mau funcionamento.
- Capacidade de autocorreção – o sistema deve ter a capacidade de identificar uma seleção de problemas e sugerir soluções.

Um ambiente inteligente é aquele que otimiza certas funções relacionadas à operação e administração de uma residência ou edifício. Portanto, automatizando os sistemas, consegue-se um aproveitamento melhor da luminosidade ambiente, controlando luzes e persianas e mantendo sempre a temperatura ideal, mas sem desperdício.

Controlando corretamente o funcionamento dos equipamentos da residência, obtém-se uma redução no consumo de energia. De Bolzani (2004, p. 49), estabelecendo uma analogia com um organismo vivo, a residência moderna parecerá ter vida própria, com cérebro e sentidos.

1.2 Motivação

Tem-se por motivação deste trabalho o desejo de obter experiência no desenvolvimento de um projeto de automação residencial, focando principalmente a área de aquisição de imagens.

Mais uma boa motivação está no apelo comercial e futurístico da idéia. Podem-se ter trabalhos futuros dando continuidade a este, visando uma versão comercial. E, a partir daí imagina-se uma empresa que implemente desde a interface até soluções de conectividade e controle de casas.

Pode-se ilustrar esse apelo futurístico na Figura 1.1, onde se tem exemplos de 4 possíveis situações em uma casa com um sistema de domótica interligado à internet.

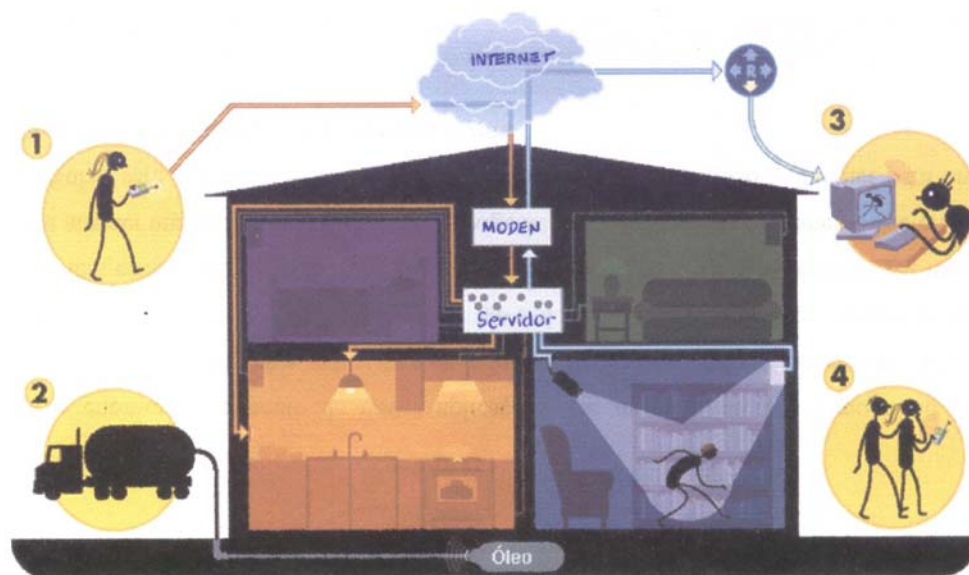


Figura 1.1 – Aplicações do projeto. Fonte: AMORY e JUNIOR, 2001

Suponha-se que Maria está saindo do seu curso (situação 1). Ela poderia usar o seu PDA (*personal digital assistant*) sem fio com acesso a internet para conectar-se a sua casa e ajustar o termostato geral e deixar a casa bem iluminada para quando chegar.

Na situação 2, o medidor de nível de óleo do sistema de aquecimento estava com nível baixo. Imediatamente o sistema manda uma mensagem para a distribuidora de óleo para que seja feito o reabastecimento.

Já na situação 3, João está trabalhando quando de repente recebe uma mensagem urgente comunicando uma invasão à sua casa. Imediatamente ele se conecta a casa e, através das câmeras de segurança, consegue ver a imagem do invasor. Instantaneamente o sistema já havia enviado uma mensagem à polícia notificando a invasão.

A situação 4, João e Maria decidem sair para viajar. Ao saírem da casa o sistema avisa ao PDA que esqueceram de ativar o alarme. Então, pelo próprio PDA, João aciona o sistema e verifica se todas as portas e janelas foram bem fechadas.

Busca-se no desenvolvimento deste projeto dar prioridade às tecnologias de baixo custo ou de livre distribuição para que uma futura comercialização do produto possa ser viável.

1.3 Estruturação do Texto

O texto foi estruturado da forma seguinte.

Neste capítulo descreve-se o histórico da automação predial e residencial e mostra-se o porquê da escolha desse tema.

O capítulo 2 é uma revisão bibliográfica, definindo conceitos que são parte integrante do trabalho como um todo.

O capítulo 3 explica a arquitetura usada, baseada em Cliente – Servidor.

No capítulo 4 relatam-se características de alguns protocolos e o porquê de estes não serem os escolhidos para o projeto.

No capítulo 5 se explica melhor o protocolo de controle escolhido, o Controller Área Network – CAN.

O capítulo 6 trata de conexões de rede sem fio. Duas tecnologias mais usuais para protocolo de controle são mais detalhadas, *Bluetooth* e *Wi-Fi*. Além disso, fala-se sucintamente de uma tecnologia que está sendo lançada agora no mercado, a *WiMax*.

Já o capítulo 7 descreve alguns conceitos diretamente relacionados às câmeras de vídeo e suas características. Também descreve como proceder para disponibilizar as imagens na internet ou intranet.

Para finalizar, o capítulo 8 cita algumas recomendações para projetos relacionados ao tema deste trabalho, mas não se contendo apenas na área residencial. São feitas considerações na mineração e no comércio também.

1.4 Objetivos

O objetivo do trabalho é o estudo do estado da arte da segurança em sistemas de automação predial, focalizando um projeto acessível e, portanto, aplicável.

Um objetivo secundário é a descrição de *cases* em outras áreas, como mineração e comércio.

2 REVISÃO BIBLIOGRÁFICA

2.1 Integração

Com o advento das redes domésticas e dos inúmeros sistemas de controle residenciais, houve a necessidade da qualificação de um profissional que atendesse as exigências do novo mercado possibilitando a criação, o desenvolvimento e a implantação dos sistemas domóticos. Em muitos casos, esse profissional iniciou sua carreira trabalhando em automação industrial desde o *hardware* básico até o gerenciamento de projetos e implantação de sistemas. A entrada no setor predial foi motivada pela necessidade de definir um nicho de mercado em que pequenas empresas pudessem atuar sem enfrentar a concorrência das grandes firmas de engenharia. O mercado de automação predial, carente de projetos e mão de obra especializada, abria espaço apenas para tecnologia vinda do exterior e específica para o setor hoteleiro e de centros de compras (*shopping centers*). Os sistemas e equipamentos utilizados até então, provenientes do ambiente industrial, eram adaptados para o setor predial. Com o crescimento do mercado de automação residencial surgiram os sistemas dedicados e a necessidade da qualificação de um novo segmento de profissionais: o integrador de sistemas residenciais.

Isoladamente cada um dos sistemas adotados em uma residência tem a sua eficiência limitada. Utilizando-se o conceito de integração, o potencial de benefícios aumenta tremendamente. A operação fica mais simples, a economia e a segurança aumentam, o conforto alastra-se pela casa toda.

A chave do processo de integração é a criação de uma adequada infraestrutura, representada pelo cabeamento e seus acessórios, responsáveis por trafegar todos os sinais de dados, voz e imagem recebidos pelas residências. E, cada vez mais, também a

tradicional instalação elétrica está sendo substituída por inovações necessárias à sua completa automação.

Em um projeto moderno, deve-se ter “centrais de distribuição” alocadas de maneira a facilitar as inevitáveis atualizações necessárias no futuro.

O diagrama da figura 2.1 exemplifica esta situação e enumera os principais sistemas domóticos passíveis de integração.

Através do diagrama percebe-se que não importa quantos diferentes produtos ou sistemas estejam envolvidos em um projeto residencial, a relação mais segura do usuário da casa com estes sistemas será através do integrador. É ele quem projeta, coordena os outros profissionais, auxilia na escolha dos equipamentos, acompanha a instalação e até mesmo presta serviços de manutenção e atualização. Segundo Bolzani (2004, p. 52), para projetar de maneira eficiente, o profissional precisa conhecer toda essa gama de opções disponíveis, identificando as necessidades e limitações do usuário e agregando todos os elementos para um projeto de sucesso.

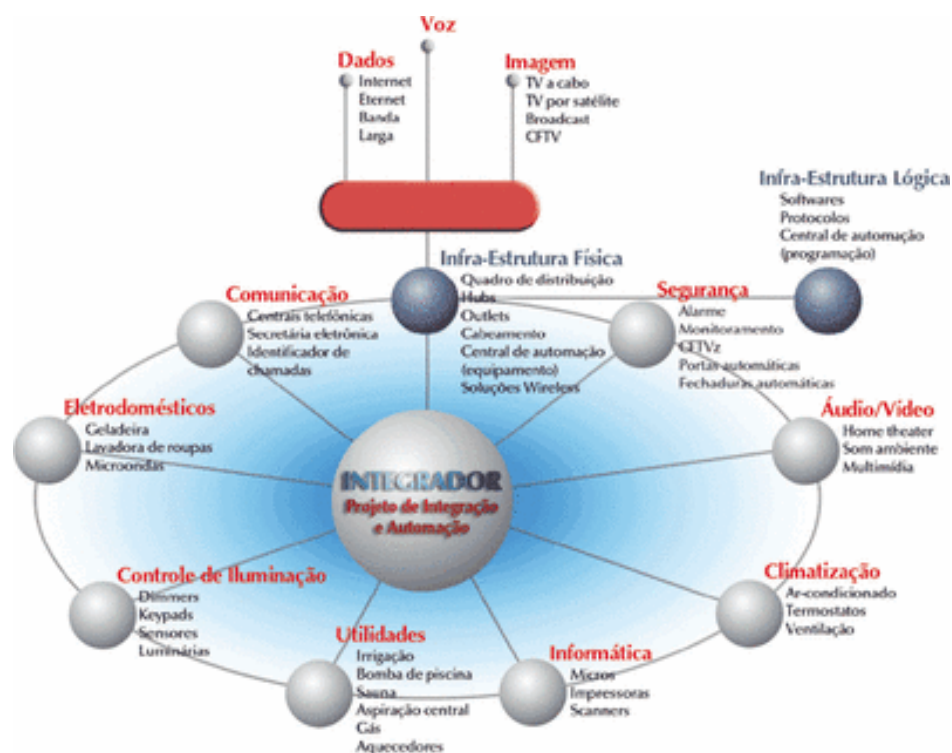


Figura 2.1 – Integrador. Fonte: AURESIDE, 2005

Atuando como elementos de integração têm as diversas opções de sistemas de automação disponíveis. Uma combinação de equipamentos e *software* adequados cria infinitas possibilidades de utilização.

2.2 Sistema

A abordagem sistêmica, estruturada a partir da década de 1950, sobretudo, da teoria geral dos sistemas - TGS, encontra seus primeiros contornos no final do século XXVII. Neste sentido Foucault (1990) observa que o conceito de organização já se mostrava visível na História Natural do século XVII. Na literatura socialista, o enfoque sistêmico “foi argumentado filosoficamente por Carlos MAX, a mais de cem anos e não só argumentado e sim aplicado ao analisar a produção capitalista, cujo fruto se conhece em EL CAPITAL”.

Foi, porém, com os estudos do cientista alemão Ludwig Von Bertalanffy (apud Alves, 2002), após a década de 1920, que a concepção sistêmica, ou de sistema, tal qual é conhecida atualmente no mundo acadêmico e da pesquisa, começa a incorporar a TGS. Portanto, baseada nas concepções de Bertalanffy (apud Alves, 2002), foi formulada a Teoria Geral dos Sistemas, visando à consecução de objetivos comuns. A partir desta abordagem, o sistema pode ser caracterizado como sendo um “conjunto de partes relacionadas, apesar de independentes, sendo, cada uma delas dependentes entre si”.

Se a Bertalanffy coube a organização dos postulados teóricos fundamentais da teoria sistêmica, sua concepção aplicativa encontrará em Shurchman o seu tradutor, conforme assinala Ribeiro (1993).

“A idéia principal de Shurchman (apud Ribeiro, 1993) é voltada para as características intrínsecas do sistema, ou seja, o todo é pensado como o objetivo central do sistema e as partes como os objetivos secundários. Esses objetivos, central e secundários, podem ser identificados como uma visão totalizante, globalizante e seu ‘repartimento’ como a capacidade que o sistema tem de se comportar e/ou decompor em subsistemas. A

idéia norteadora é o aspecto planejamento-controle com vistas à sua finalidade única: a eficiência do todo e das partes que compõem esse todo para alcance de um fim proposto”.

A teoria dos sistemas possui também seus críticos, notadamente quando a mesma é utilizada indiscriminadamente.

Castro (1986), afirma: “*O enfoque sistêmico pode ser analisado no sentido mais amplo ou restringi-lo a certas situações*” Em seu sentido mais restrito o mesmo está vinculado ao conhecimento de uns ou outros objetos e fenômenos da realidade. Ainda segundo Castro (1986), “*os teóricos burgueses o apresentam como uma filosofia especial, como um fundamento metodológico da ciência e até como uma nova concepção do mundo, algo assim como ‘a chave mágica, capaz de abrir a plenitude das riquezas da realidade’*”.

2.2.1 O Enfoque Sistêmico Adotado

O presente trabalho tem como objetivo caracterizar as condições físicas de prédios e formular propostas para torná-lo inteligente, buscando alcançar uma maior eficiência, qualidade e confiabilidade do processo de automação. Para esses objetivos é que se propõe a utilização do enfoque sistêmico.

Em Castro (1986), tem-se o enfoque sistêmico se apoiando na categoria filosófica do geral e do particular, que expressa “*a relação dos conjuntos de objetos e o nexos que os une, fazendo aparecer novas propriedades e regularidades não inerentes aos objetos isolados, tendo como particularidade o nexos que os une determina as características do todo, além de se sustentar no conceito da unidade material do mundo*”.

Concordando com Castro (1986), será adotado o enfoque sistêmico na justa medida; nele será adotada a “categoria filosófica do particular”, ou seja, será abordado o sentido mais restrito, vinculado ao conhecimento de objetos e fenômenos da realidade.

Não esquecer, porém, que todo sistema convenientemente determinado, se compõem de múltiplos subsistemas e estes, por sua vez, de tantos outros quanto a sua natureza o permita.

2.2.2 Propriedade do Sistema

Será adotado o critério de Victor Afanasiev, citado por Castro (1986), para descrever as quatro propriedades do sistema: Componentes, Estrutura, Funções e Integração.

Componentes são os elementos que constituem o sistema e suas relações;

Estrutura é o modo de interconexão dos componentes do sistema;

Funções são as ações que um sistema pode desempenhar, tanto de subordinação vertical como de coordenação no sentido horizontal;

Integrações são os seus mecanismos, os quais asseguram a sua pedurabilidade e se apóiam na cibernética e na direção.

2.2.2.1 Componentes Propostos

Cada variável CFTV, controle de acesso, iluminação se relaciona e se complementa e quando em seus corretos valores, resguarda o perfeito funcionamento do prédio inteligente; portanto, constituem os componentes do sistema proposto.

2.2.2.2 Estrutura

Os componentes em investigação, CFTV, controle de acesso, iluminação se relacionam e se interconectam de forma a se complementarem e também, quando em seus valores corretos garantem as condições ideais para o desenvolvimento otimizado da automação. Qualquer alteração significativa em um dos componentes afeta o desempenho

global do sistema; por exemplo: a falta de identificação no CFTV poderá não abrir uma porta de acesso.

2.2.2.3 Funções

As ações que o sistema pode desempenhar, tanto de subordinação vertical como de coordenação no sentido horizontal, ficam explicitadas na forma que este pode, quando colocado em prática, influenciar a automação positivamente quando em equilíbrio ou, negativamente quando qualquer um de seus componentes extrapola seus valores ideais. A subordinação vertical na busca da condição ideal depende da coordenação horizontal da interconexão entre seus componentes.

2.2.2.4 Integração

A integração que se dá através da boa comunicação entre os seus componentes e de um controle adequado, garantindo a direção necessária para as condições mais favoráveis ao desenvolvimento da automação. É condição necessária e fundamental a atuação integrada dos componentes de forma a permitir que o comportamento do sistema atue conforme previsto e ou planejado.

2.2.3 Conclusão sobre o Enfoque Sistêmico Adotado para esta Investigação.

Fica evidenciado que para esta investigação, o conceito de um sistema vinculado ao conhecimento de objetos e fenômenos da realidade, ou seja, “uma categoria filosófica particular”, será de grande valia para o processo de automação.

2.3 Domótica

Originado na França, a partir do surgimento de disciplinas acadêmicas e desenvolvimento de pesquisas nas áreas de tecnologia de automação residencial e comunicação de dados, o termo Domótica (do francês “Domotique”) é usado para designar toda residência que emprega serviços automatizados relacionados à gestão de energia, comunicação, conforto ambiental, segurança pessoal e patrimonial. Segundo Mariotoni e Junior (2001, p. 1), tem-se uma definição mais técnica para o termo Domótica dizendo que uma rede domótica seria representada por um conjunto de serviços de uma residência assistidos por um serviço que interliga e realiza várias funções de gerenciamento e atuação, podendo estar conectadas entre si por meio de uma rede de comunicação interna e ou externa oferecendo um conjunto de aplicações.

A domótica pode substituir o homem em diversas atividades rotineiras de forma a proporcionar uma otimização nas condições de vida de uma casa. O próprio sistema zela pela satisfação dos moradores, sem que seja necessária a contínua intervenção dos mesmos.

O grau de controle alcançado pode ser variável, sendo uma função de custo, desejo pessoal dos moradores, estrutura do prédio e tecnologia usada. Casas que podem ter, por exemplo, ajuste automático de temperatura, escalonamento automático de tarefas rotineiras como ligar a cafeteira, acionamento automático dos serviços de segurança e

comunicação eficiente com o mundo externo têm vários benefícios que serão descritos posteriormente.

De uma maneira geral um sistema domótico será composto de uma rede de comunicação que permite uma interconexão de uma série de equipamentos com o objetivo de obter informações do ambiente residencial, e efetuando determinadas ações nesse com o objetivo de gerenciá-lo. Haverá elementos de campo (detectores, sensores e captadores) transmitindo informações para as unidades centrais inteligentes que se encarregarão de processar os dados recebidos e como consequência efetuar o acionamento de determinados equipamentos ou gerar alertas de aviso. Com isso a unidade central de processamento irá atuar sobre o sistema e seus circuitos correspondentes, com o objetivo de corrigir as falhas encontradas. Os tipos de comandos de acesso aos serviços de uma rede domótica caracterizam-se por fornecer aos usuários diferentes formas de controle e gerenciamento da rede. Essas formas de controle dividem-se de acordo com o tipo de equipamento a ser acionado ou programado, e com o serviço a ser acessado pelo usuário. Podem ser de controle interno, controle externo, programabilidade e acesso remoto (utilização de redes de comunicação externa para acesso à residência, ou a partir da residência a utilização de serviços externos como bancos, concessionárias de serviços públicos e privados, etc.).

De acordo com Mariotoni e Junior (2001, p. 2), um sistema domótico deve priorizar alguns aspectos de implantação e manutenção que serão apontadores de qualidade, integração e operabilidade e farão com que o sistema funcione de forma realmente integrada e inteligente, são eles:

- Seleção do tipo de usuário;
- Possibilidade de realizar pré-instalações do sistema na fase de construção da residência;
- Facilidade de ampliação e incorporação de novas funções;
- Simplicidade de uso;
- Nível de normalização e implantação do sistema;
- Variedade de elementos de controle e funcionalidade disponíveis;
- Critérios técnicos;
- Tipo de arquitetura de rede e topologia de distribuição;

- Velocidade de transmissão;
- Protocolo de comunicação.

As redes domóticas se encarregam de gerenciar principalmente os serviços de economia de energia elétrica, segurança, comunicação e conforto. O controle do consumo de energia elétrica é realizado através da implantação de temporizadores, relógios programadores, sensores e termostatos, aproveitando-se também da tarifação diferenciada quanto da utilização de equipamentos fora de horários de pico. A rede proporciona uma série de comodidades de controle e conforto através da automação das instalações e serviços de aquecimento, condicionamento e iluminação, podendo ainda controlar elementos como janelas, persianas e toldos. Pode-se ter através da rede o gerenciamento e controle sobre o acesso à residência seja interno ou externo, promovendo a segurança patrimonial. Também se tem opções para a monitoração das ações de crianças, idosos e pessoas doentes presentes na residência. O serviço de comunicação talvez seja o ponto mais importante da rede domótica, pois é através deste que irão trafegar os dados de avaliação e controle e também os comandos de acionamento de equipamentos e serviços diversos.

De acordo com Amory e Junior (2001, p. 2), outro termo importante a se definir é o conceito de teleação, que é a capacidade de se controlar algum dispositivo remotamente. A Figura 2.2 ilustra este conceito.

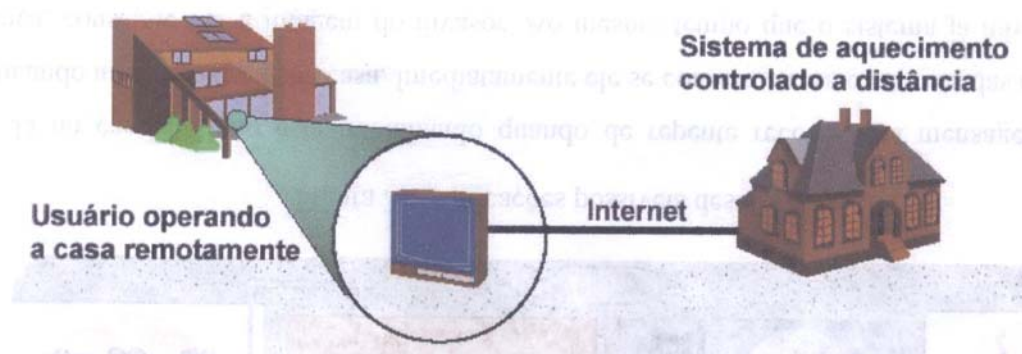


Figura 2.2 – Teleação. Fonte: AMORY e JUNIOR (2001, p. 2)

Com a junção da domótica e teleação surgiu a idéia de interligar a rede interna de uma casa (domótica) com a rede externa à casa (Internet) para que os moradores possam controlar, monitorar e principalmente administrar seu lar à distância.

2.3.1 Benefícios da Domótica

De acordo com os conceitos de Amory e Junior (2001, p. 5), os benefícios da domótica concentram-se em quatro classes: segurança, conforto, economia de energia e comunicação. Pode-se exemplificar cada ponto desse.

2.3.1.1 Segurança

Trata de proteger pessoas e pertences em casos de eventualidades como invasão, vazamento de água, incêndio, doenças, etc. Pode-se destacar como aplicações:

- Alarmes técnicos: inundação, gás, queda de energia;
- Fogo e fumaça: detecção rápida, alerta a moradores, chamada de bombeiros;
- Invasão e assalto: comunicação à polícia, sistema de câmeras, foto das pessoas que passaram pela frente da porta dianteira ou tocaram a campainha;
- Alarme médico: monitoramento e diagnóstico remoto de sinais vitais;
- Simulação de presença: ligar música e luzes aleatoriamente.

2.3.1.2 Conforto

Exemplificam-se alguns controles relacionados ao conforto das pessoas da residência automatizada:

- Luz automática: acionamento por presença, som, hora ou luz ambiente;
- Persianas: controle automático por presença de luz ambiente e chuvas, abertura automática de persianas pelo acionamento do despertador;
- Centralização: ligar ou desligar o sistema com um único botão;
- Controle de temperatura: temperatura interna mantém-se sempre a um nível agradável;
- Programação de eletrodomésticos: pode-se programar para que a cafeteira e o aquecimento da banheira liguem 10 minutos antes que o despertador seja acionado;
- Abertura de portões.

2.3.1.3 Energia

Controles inteligentes podem evitar desperdício de energia, exemplificando:

- Iluminação: desliga luzes automaticamente quando não houver pessoas em determinado ambiente;
- Controle de temperatura: poder controlar aquecedores e ar condicionado de forma a minimizar o consumo de energia;
- Controle de eletrodomésticos: acionar eletrodomésticos como lavadoras de roupa em horários que as tarifas são menores ou fora de horários de pico.

2.3.1.4 Comunicação

- Segurança: chamada automática a bombeiros e polícia;
- Entretenimento: interligação de áudio e vídeo, sinal de videofone na televisão;
- Conectividade: interligação entre casas, escritórios, prédios que utilizam a domótica (WAN).

2.4 Segurança

Nos dias de hoje, o setor de segurança anda a passos largos em direção a uma melhor qualidade e profissionalização. O emprego de sistemas eletrônicos de segurança já se tornou comum, pelo menos nas grandes cidades onde a população não teve outra escolha senão se proteger e aderir à presença constante de câmeras e demais formas de monitoramento.

Indústrias, *shoppings* e bancos, visando aumentar a segurança de usuários e clientes, já dispõem de modernas centrais de monitoramento, em que sistemas de alarmes conjugados a câmeras possibilitam não só gravar imagens de eventos suspeitos como também acionar mecanismos de defesa após a identificação de um sinal de invasão enviado a uma central de monitoramento.

Segundo Manger (2004, p. 19), são muitos os recursos tecnológicos voltados para a segurança predial que estão disponíveis hoje: controle de acesso de pessoas e veículos com o uso de cartões magnéticos, sensores de proximidade, teclado de código, leitura de íris (substituindo as impressões digitais, determinando abertura e fechamento de portas). Nos edifícios mais sofisticados, o acesso pode ser restringido a alguns horários, ou seja, a utilização de uma sala pode ser permitida em determinadas horas e situações. Além

de gerenciamento centralizado, câmeras de segurança, alarme de incêndio, alarme patrimonial, sistemas de segurança, videoconferência, tele vigilância.

Todo o sistema de segurança é complementado pelo de telecomunicações/telemática, onde os dados são obtidos e transferidos.

De acordo com Bolzani (2004, p. 65), para se realizar um bom projeto de segurança patrimonial em uma residência é imprescindível criar soluções que sejam não somente compatíveis, mas também complementares, além de cumprir fundamentalmente os seguintes pontos, considerados básicos em um sistema com tal propósito:

- Prevenção ou dissuasão – utilização de sistemas que inibam e promovam a desistência da ação de intrusão;
- Detecção e alarmes – utilização de sistemas que permitam a detecção de ações de intrusão e possibilitem o acionamento de diversos tipos de alarmes;
- Reconhecimento ou identificação – a residência inteligente deve ser capaz de tomar decisões e cumprir processos baseados no reconhecimento e identificação do usuário;
- Reação – o sistema deve realizar as funções de reação, disparando ações contra o processo de intrusão.

No controlador central, o tratamento dos sensores proporciona informações claras e objetivas ao usuário, tanto do estado das instalações como também dos eventos que vão se produzindo. Existem dois cenários básicos com que o sistema deve lidar: quando o usuário está em casa e quando não está. O *software* deve ser capaz de prever várias situações de ataque e reação a fim de nunca deixar o usuário em posição de risco.

Resumindo, a evolução do setor de segurança antecipa uma situação já esperada: a alta tecnologia por toda à parte. Com os lançamentos cada vez mais sofisticados, profissionais do ramo podem cada vez mais oferecer soluções para problemas que afligem toda a sociedade.

3 ARQUITETURA DO SISTEMA

Como o projeto proposto tem a idéia de um posterior monitoramento de toda a residência via internet, o sistema terá a comunicação baseada no protocolo http, onde um dos computadores é denominado servidor e o(s) outro(s) cliente(s). Interligando os periféricos da casa internamente tem-se outra rede, utilizando o protocolo *Controller Área Network* - CAN. Esta rede utiliza um controlador mestre para se comunicar com o servidor, o que é feito através da porta RS-232. A figura 3.1 mostra uma idéia geral da arquitetura do sistema.

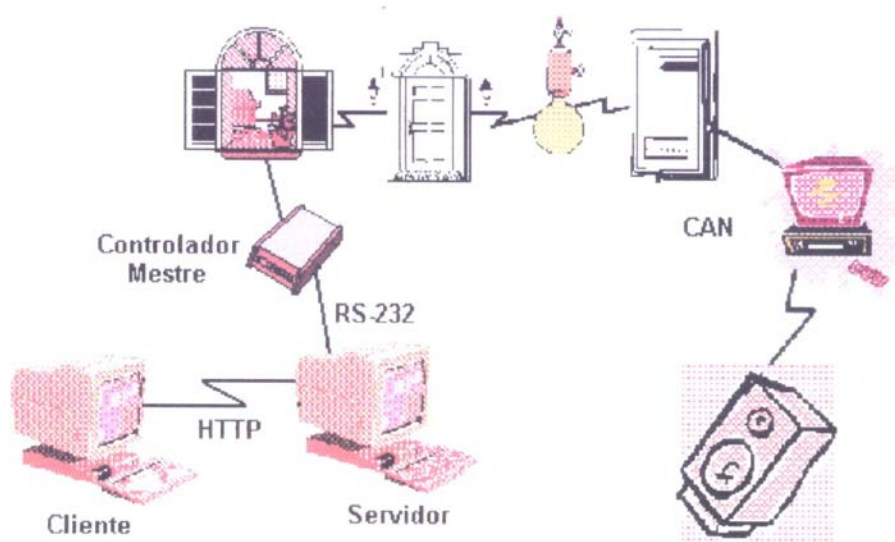


Figura 3.1 – Arquitetura do Sistema. Fonte: AMORY e JUINOR (2001, p. 9)

No(s) micro(s) denominado(s) cliente(s) – responsável por permitir que o usuário interaja amigavelmente com sua residência – tem-se um *software* que será o navegador *Web*, responsável pelo envio de sinais de controles. Estes sinais, que se denomina de pacotes de controle serão recebidos pelo servidor para serem tratados de forma adequada.

O servidor, interpretando estes pacotes, é responsável por atualizar um banco de dados e repassá-los, através da porta RS-232, para o controlador mestre da rede interna da casa.

O controlador mestre da rede residencial fará a codificação dos dados recebidos pelo servidor para o protocolo CAN. Além disso, tarefas como endereçamento dos pacotes, gerenciamento do barramento e decodificação dos dados recebidos dos periféricos para o servidor, também são tarefas do controlador mestre.

Enquadra-se como responsabilidade do servidor a atualização, de maneira transparente ao usuário, da interface do navegador *Web* (cliente). Em outras palavras, isso possibilita que o usuário tenha sempre o último estado sobre sua residência sem a necessidade de ficar acionando um comando de atualização da interface.

A idéia mais simples é instalar uma rede serial na casa. Esta interligará todos os periféricos e nela tráfegarão os comandos e dados necessários para automação da casa. Estes periféricos serão controlados pelo controlador mestre que por sua vez recebe comandos do servidor.

4 PROTOCOLO DE CONTROLE

Hoje existem vários protocolos de comunicação, que são impulsionados devido à demanda de comunicação e fluxo de informações. Esses protocolos devem ser escolhidos de acordo com a área de aplicação.

Aqui se relatam as características de alguns protocolos de controle e o porquê de não serem escolhidos.

4.1 Introdução

Segundo Amory e Junior (2001, p. 23), protocolo é a especificação de um conjunto de regras que diversos equipamentos respeitam para trocar informações. São usados como linguagem de comunicação entre os módulos processadores responsáveis pelo controle de atuadores e monitoração de sensores.

Com o crescimento da automação e da tecnologia dos dispositivos, a área de protocolos de controle tem crescido bastante.

Com esse aumento de mercado a solução que todos buscam é a padronização das interfaces de comunicação, para se ter mais competitividade e flexibilidade para os consumidores.

4.2 Características e Requisitos de Protocolos

A aplicação do projeto é o que define as características a serem estudadas do protocolo de controle. Por exemplo, quando se procura por um protocolo para ser usado em uma grande indústria metalúrgica, esse protocolo deve ter longo alcance para poder se estender por toda empresa, poder ligar vários nodos, ter grande imunidade a ruídos, usando técnicas de detecção e correção de erros, terem alta disponibilidade e tolerância à falhas, uma vez que grandes valores e vidas humanas podem estar em jogo. Já um protocolo para aplicação basicamente dentro do ambiente doméstico, não necessita ter alta disponibilidade, precisa ter grande taxa de transferência para transportar vídeo e som, um alcance curto já será o suficiente, compatibilidade entre vários fabricantes, entre outras características.

Segundo Amory e Junior (2001, p. 26), além dessas características específicas de cada projeto, também deve-se levar em consideração:

- Custo/benefício da técnica de cabeamento. A técnica de cabeamento e conexão é um dos itens que mais influenciam no custo total de instalação de uma rede;
- Custo de manutenção e facilidade de diagnosticar problemas;
- Confiabilidade – as técnicas de detecção e correção de erros são adequadas a sua aplicação? O ambiente onde a rede será instalada possui muito ruído? Confiabilidade pode ser aplicada aos dados, com técnicas como CRC, e no meio de comunicação;
- Flexibilidade – capacidade de modificação do *layout* do sistema;
- Compatibilidade – é importante que vários fabricantes suportem o protocolo escolhido para que você não fique dependendo de um só fabricante, tendo maior liberdade de escolha de equipamentos e de suporte técnico.
- Parametrização – corresponde à facilidade de inserção de novos nodos na rede;
- Variabilidade de aplicações – o mesmo protocolo pode ser empregado em aplicações diferenciadas?
- Interface com PC;
- *Drivers de hardwares e softwares;*

- Taxa de comunicação – a taxa mínima de comunicação do protocolo é compatível com o tempo de resposta?
- A rede será multi-mestre ou com um único mestre? Uma rede que suporta múltiplos mestres tem uma maior disponibilidade. Em uma rede com um único mestre corre-se o risco de, se o mestre falhar, todo o sistema entrar em colapso;
- Topologia – barramento, anel, estrela, hierárquico, entre outros. Topologia está relacionada com o número máximo de nodos da rede e com o comprimento máximo;
- Resposta em tempo real
- Requisição remota – um nodo pode pedir um dado para outro nodo na rede. Essa característica é útil para se verificar se um nodo está em funcionamento;
- Sincronização inter-processador – deve-se manter sincronismo em uma rede onde dispositivos possuem velocidades diferentes;
- Comprimento físico da rede;
- Número de *bytes* de dados – número máximo de *bytes* que um pacote pode transmitir;
- Facilidade de integração – é um item relacionado ao custo total do sistema;
- Maior aceitação no mercado – é mais fácil encontrar suporte técnico;
- Padronização – verificar se o protocolo estudado é padronizado;
- *Plug and play* – maior facilidade de instalação;

4.3 Protocolos analisados

Abaixo apresenta-se uma tabela com alguns protocolos e as características primordiais de cada um deles para aplicação em um projeto de automação predial.

Tabela 4.1 – Tabela comparativa entre protocolos

| | LON | CEBus | EIB | DLC | EHS | X-10 |
|---------------------------------------|------------------------|----------------------------|------------------------|------------|------------------------------|------------------------|
| Taxa de Tx | 78Kbps a 1,25Mbps | * | 9,6Kbps | 10,4Kbps | * | * |
| Nro Max nodos | 32385 | * | 11520 | * | * | * |
| Método acesso ao Meio | CSMA Controlado | * | CSMA/CA | CSMA/CD | CSMA | * |
| Alcance | 1300m | * | 1000m | * | 350m | * |
| Aberto | Não | Sim | * | * | Sim | Não |
| Aplicação Típica | Automação Doméstica | Automação Doméstica | Automação Doméstica | Automotiva | Automação Doméstica | Automação Doméstica |
| Topologia | Hierárquico | * | Hierárquico | Barramento | Barramento Em níveis | * |
| Métodos de Verificação de Erros | * | * | Checksum | CRC | CRC e FEC para PL | Comple- mento |
| Flexibilidade dos Pacotes | * | Muito Boa | Boa | Boa | Muito Boa | Ruim |
| Complexidade de Implementação | * | * | * | Pequena | Alta | Peque- na |
| Plug and Play | Não | Sim | Não | Não | Sim | Sim |
| Padrão | Não tem | EIA-600 | Não tem | SAEJI850 | Encaminha do | * |
| Meios Físicos Suportados | NPT,CX, PL,RF e IR | PT,CX,PL, RF,IR e FO | PT,PL, RF | Serial | PT1,PT2, PL,RF,CX e IR | PL |

* Documentação encontrada não foi suficiente para julgar este item

** Tabela 2

Tabela 4.2 – Legenda da tabela comparativa de protocolos

| Sigla | Legenda |
|-------|------------------|
| PT | Par trançado |
| CX | Cabo coaxial |
| PL | Linha de energia |
| RF | Rádio frequência |
| IR | Infra vermelho |
| FO | Fibra ótica |

Analizando a tabela 1 e a bibliografia estudada identifica-se o porquê de esses protocolos não serem os escolhidos.

- *European Home Systems* - EHS – é um protocolo criado baseado nos requisitos e restrições que a automação doméstica exige. Porém, percebe-se que se trata de um protocolo muito amplo e com várias camadas de implementação (aplicação, rede, enlace e físico), por esse motivo não será o protocolo selecionado para este projeto.
- *Byte Data Link Controller* – BDLC – apesar de se encontrar documentação completa, gratuita, incluir fluxogramas e ser simples de implementar, o que mais desmotivou a usar esse protocolo é sua baixa taxa de transferência de dados. Com uma taxa de 10,4 Kbps ficaria impossível manter o compromisso de desenvolver um protocolo versátil para domótica. Aplicações como transferência de imagem seria prejudicada por essa baixa taxa.
- *Local Operating Network* – LON – como vantagens desse protocolo destacam-se a taxa de transferência, a estrutura hierárquica e o uso de linha de energia como meio físico. Porém sua desvantagem é o algoritmo simples de acesso ao barramento e o fato de ter mestre único. O fato de ser um protocolo proprietário da Echelon e ter pouca documentação especificando o protocolo completa as desvantagens.
- *European Installation Bus* – EIB – o ponto forte desse protocolo é o método de acesso ao meio, que possibilita o uso em aplicações críticas em tempo real. Porém o que nos levou a rejeitar esse protocolo foi a falta de literatura detalhada que especificasse o protocolo, o fato de ser um protocolo mais restrito à Europa e a taxa

de transferência de 9600bps. Também relata-se que equipamentos que utilizam esse protocolo são em torno de 10 a 100 vezes mais caros que equipamentos similares.

- X-10 – as grandes vantagens do protocolo X-10 são sua simplicidade e o uso da linha elétrica como meio físico. Isso leva a uma diminuição de custo de implementação e facilidade de manutenção e instalação, o que muitas vezes pode ser feito pelo próprio consumidor. Essas vantagens foram marcantes para X-10 ser o protocolo específico para automação doméstica mais famoso e usado. Porém, opta-se por não escolhê-lo justamente por ser simples ao ponto de dificultar o uso deste protocolo para aplicações mais exigentes, onde uma alta taxa de transmissão é exigida.
- *Consumer Electronics Bus* – CEBus – pareceu ser um protocolo muito bem especificado, visando o crescimento futuro que o ramo de automação doméstica está tendo. Sua flexibilidade e facilidade de instalação são o seu diferencial. Porém a escassez de material técnico gratuito impossibilitou maiores análises do protocolo.

Pode-se concluir que seria possível o uso de alguns dos protocolos citados, porém, como se tem a possibilidade de utilizar o CAN – que não têm muitas destas restrições – opta-se por ele.

5 *CONTROLLER AREA NETWORK – CAN*

5.1 Aplicações

Uma das principais preocupações que se teve para escolher o protocolo a ser implementado foi a flexibilidade em nível de aplicações que ele pode ter. Por esse motivo, escolheu-se um protocolo que não restringe a aplicações somente ao âmbito deste projeto, para que se no futuro o projeto for utilizado para fins comerciais, seja fácil a sua ampliação.

5.2 Conceitos Básicos

A escolha do CAN se deu por suas características que, de acordo com Amory e Junior (2001, p. 44), são:

- Priorização de mensagens;
- Garantia do tempo de latência (tempo real);
- Flexibilidade de configuração;
- Recepção multicast com sincronização;
- Varias técnicas para manter consistência de dados;
- Multi-mestre;
- Técnicas de detecção e sinalização de erros;
- Desligamento automático de nodos com defeitos.

O barramento CAN possui dois valores. O Dominante, equivalente ao nível lógico 0 (zero) e o Recessivo, equivalente ao nível lógico 1 (um).

Existem duas especificações sobre o protocolo CAN. A primeira é chamada *Standard CAN* e a segunda *Extended CAN*. A tabela faz um comparativo entre as duas especificações.

Tabela 5.1 – Comparativo entre CAN padrão e estendido

| | Standard CAN | Extended CAN |
|--|--------------|--------------|
| Nome da Especificação | CAN 2.0 A | CAN 2.0 B |
| Número de bits do campo de identificação | 11 | 29 |

5.2.1 Formato dos Pacotes

Cada mensagem CAN consiste em uma sequência de *bits* que é dividida em campos. Cada campo tem uma função diferente como descrita a seguir.

CAN possui quatro tipos de mensagens: dados, requisição remota, erro e *overload*. O formato e função de cada pacote é explicado a seguir.

5.2.2 Pacote de Dados

A figura 5.1 ilustra o formato do pacote de dados CAN.



Figura 5.1 – Formato de um pacote de dados CAN. Fonte: AMORY e JUNIOR (2001, p. 46)

Define-se cada campo como:

- SOF – 1 bit – dominante – marca o início de uma mensagem. Quando o barramento se encontra ocioso, uma borda de descida do SOF sincroniza os nodos de rede.
- Arbitração e Controle – esses campos são subdivididos de acordo com a figura 5.2.

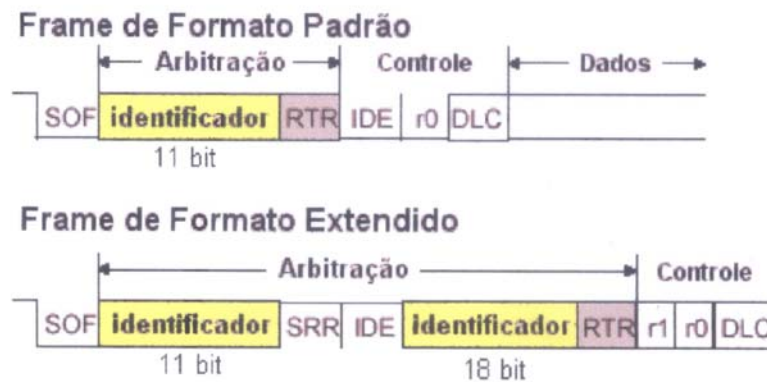


Figura 5.2 – Campo de arbitração. Fonte: AMORY e JUNIOR (2001, p. 46)

- Identificador – 11 ou 29 *bits* – é o endereço lógico e a prioridade da mensagem. Valores menores têm maior prioridade. O formato padrão possui 11 *bits*, enquanto o estendido possui 29.
- RTR – 1 *bit* – o RTR (*Remote Transmission Request*) identifica se a mensagem é de dados (dominante) ou de requisição de dados (recessivo).
- IDE – 1 *bit* – o IDE (*Identifier Extension*) identifica se a mensagem é do formato padrão (dominante) ou estendido (recessivo).
- SRR – 1 *bit* – recessivo (*Substitute Remote Request*).
- r0 e r1 – 2 *bits* – dominantes. São *bits* de reserva
- DLC – 4 *bits* – O DLC (*Data Length Code*) informa o número de *bytes* que será transmitido. Originalmente CAN suporta o envio de até 8 *bytes* de dados em um único pacote. Porém, em aplicações específicas, pode-se fazer uso de até 16 *bytes* de dados por pacote.
- Dados – 0 a 64 *bits* – contém o dado da mensagem

- CRC – 16 *bits* – CRC contém o *checksum* dos *bits* precedentes da mensagem. O *checksum* é usado para detectar erros.
- ACK – 2 *bits* – é composto pelo *bit* ACK *Slot* e pelo *bit* Delimitador e ACK. Transmissores enviam ambos os *bits* em recesso. Um receptor indica que recebeu a mensagem enviando um *bit* dominante no ACK *Slot*. Isso indica ao transmissor que ao menos um nodo recebeu a mensagem corretamente.
- EOF – 7 *bits* – todos recessivos – EOF (*End Of Frame*) delimita o fim de uma mensagem.
- IDLE – 0 ou mais *bits* – recessivos – sinaliza que o barramento está livre. Qualquer nodo pode começar uma transferência de mensagem
- *Intermission* ou IFS (*InterFrame Space*) – 3 *bits* – recessivos – IFS é o tempo necessário para que um nodo transfira um pacote corretamente recebido no barramento para área de armazenamento local (*mailbox*). É o tempo mínimo entre a transmissão de dois pacotes.

5.2.3 Pacote de Requisição de Dados

Existe a possibilidade de um nodo de destino requisitar dados da origem. Para isso o nodo de destino envia uma requisição de dados (RFR – *Remote Frame Request*) com o identificador que pertence ao dado requerido. O nodo que tem este dado devolverá um pacote de dados, respondendo à requisição.

A figura 5.3 ilustra o funcionamento de RFR. O nodo 1 envia uma requisição de dados com o identificador do mesmo, indicado pela marca (1) na figura. O nodo que responde por esse dado (identificador) é o nodo 2. O nodo 2, então, envia o dado requisitado (marca (2)) ao barramento e os nodos 1 e 4 lêem este dado (marca (2)).

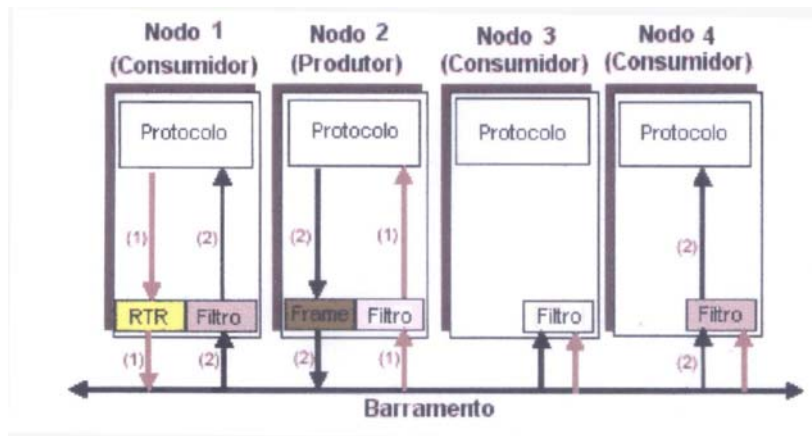


Figura 5.3 – Requisição remota de dados. Fonte: AMORY e JUNIOR (2001, p. 48)

Existem duas diferenças entre pacotes de dados e pacotes RFR. Primeiramente o *bit* RTR é transmitido dominante em pacotes de dados e recessivo em RFR. A outra diferença é que não existe campo de dados em RFR. Quando um pacote de dados e um RFR com mesmo identificador são transmitidos no mesmo instante, o pacote de dados ganha a disputa devido ao *bit* RTR dominante. Assim, o nodo que requisitou o dado recebe-o imediatamente. A figura 5.4 ilustra o formato deste pacote.

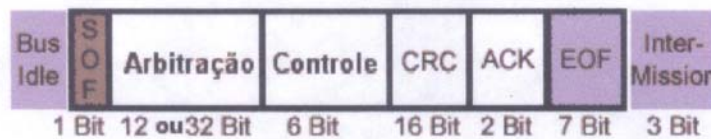


Figura 5.4 – Pacote de requisição de dados CAN. Fonte: AMORY e JUNIOR (2001, p. 49)

5.2.4 Pacote de Erro

De acordo com Amory e Junior (2001, p. 50), um pacote de erro é gerado por qualquer nodo que detecte um erro. Sua função, portanto, é notificar a ocorrência de falhas. O pacote de erro é formado por dois campos: *flag* de erro e delimitador de erro. A figura 5.5 mostra o formato do pacote de erro.

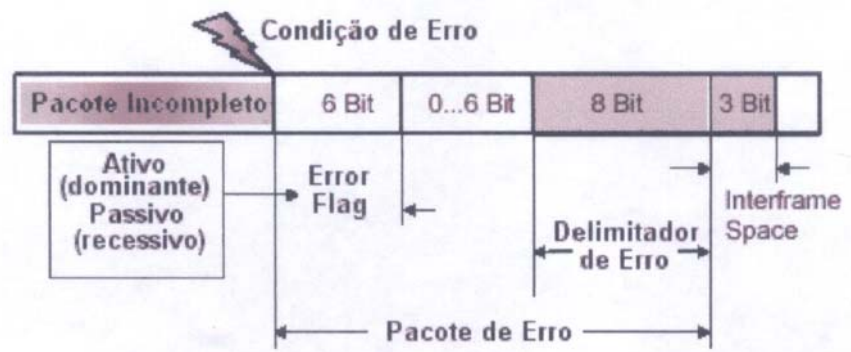


Figura 5.5 – Pacote de erro CAN Fonte: AMORY e JUNIOR (2001, p. 49)

Definem-se os campos como:

- *Flag* de Erro – 6 *bits* – é o campo que sinaliza a existência de um erro. Existem dois tipos de *flag* de erros: *flag* erro ativo e *flag* erro passivo. Um nodo em estado de erro ativo envia um *flag* de erro ativo (dominante), enquanto um nodo em estado de erro passivo envia um *flag* de erro passivo (recessivo).

O campo de *flag* de erro é enviado pelo nodo que detectou o erro e, se esse nodo estiver em estado ativo (dominante), sobrescreverá o dado corrompido. Quando os outros nodos da rede recebem a sequência de 6 *bits* dominantes referente ao *flag* de erro, irá ocorrer uma violação de *bit stuffing* e todos os nodos enviarão ao mesmo tempo um outro *flag* de erro. Os próximos 6 *bits* são esse segundo *flag* de erro que é enviado, em dominante, pelos outros nodos da rede.

Se o nodo que identificou o erro está em modo erro passivo, ele enviará um *flag* de erro recessivo e mais o delimitador, também em recessivo. Portanto erros sinalizados por nodos em estado de erro passivo não afetarão o barramento, isolando assim nodos que tenham uma taxa de erros grandes.

- Delimitador de Erro – 8 *bits* (recessivo) – é transmitido pelo nodo que enviou o dado que continha erro. Sua função é recomençar comunicação no barramento após uma falha.

5.2.5 Pacote de *Overload*

É usado, basicamente, para sinalizar a um transmissor que o receptor não está pronto para receber as próximas mensagens, portanto o transmissor deve esperar para fazer a próxima transmissão.

O formato do pacote é idêntico ao pacote de erro com a diferença que *Overload Flag* é sempre dominante e que o envio de um pacote de *overload* ocorre sempre após os 3 *bits* de IFS, ou seja, depois do fim de uma mensagem.

5.2.6 Arbitração

De acordo com os conceitos de Amory e Junior (2001), se dois ou mais nodos começam a transmissão no mesmo instante, a colisão das mensagens é evitada pela implementação do protocolo CSMA/CD+AMP para decidir disputas de acesso ao barramento. O campo de identificação dos pacotes conterá não somente a identificação do dado, mas também a prioridade que essa mensagem terá. Identificadores de menor valor terão maior prioridade.

Enquanto os nodos estiverem enviando os mesmos *bits* de identificação, nada acontece. No entanto, quando um nodo enviar um *bit* de identificação de prioridade menor, esse perderá a disputa pelo barramento.

5.2.7 Bit-Timing

Um *Bit Time* é o período de transmissão e recepção de um *bit*. Todos os nodos da rede devem ter o mesmo *bit time*. *Bit time* é formado por quatro segmentos. Cada segmento é formado por múltiplos *Time Quantum* (tq). O *Time Quantum* é uma unidade de tempo fixa (menor porção do tempo usada no nodo CAN) derivada do *clock* do sistema.

5.2.8 Sincronismo

Duas técnicas de sincronização são suportadas: *Hard Synchronisation* e *Soft Synchronisation*.

- *Hard*: é acionado na borda de descida quando o barramento está livre, que é interpretado como SOF. Essa sincronização inicia a lógica interna de *bit time*.
- *Soft*: é usado para ajustar o *bit time* enquanto o nodo CAN está recebendo um pacote. Quando o transmissor é lento em relação ao receptor o *bit time* é aumentado. Quando o transmissor é mais rápido o *bit time* é diminuído.

5.3 Camada Física

A fiação do barramento CAN é feita a dois fios: CAN-L e CAN-H. Essa técnica é usada para minimizar efeitos de interferências eletromagnéticas no barramento.

CAN usa a técnica de sinalização por tensão diferencial. Isso quer dizer que o nível do sinal, dominante ou recessivo, é determinado pela diferença de tensão entre

CAN-H e CAN-L. Em nível recessivo, CAN-H não pode ter uma tensão maior que 0,5V em relação à tensão CAN-L. Se a tensão CAN-H for pelo menos 0,9V maior que CAN-L, então o barramento está em nível dominante.

Com esta técnica de fiação consegue-se minimizar efeitos de interferência eletromagnética porque essa interferência vai afetar ambos os fios CAN-L e CAN-H da mesma forma, permanecendo a tensão diferencial igual.

Para se fazer a interface do controlador CAN com o barramento é necessário que exista um *transceiver* para fazer a codificação do sinal do controlador para sinal de tensão diferencial do barramento.

A taxa de transferência máxima de uma rede CAN é de 1Mbit/s. Porém essa taxa varia de acordo com o comprimento da rede, devido à resistência dos fios do barramento.

6 CONEXÕES

6.1 Tecnologia Bluetooth

Em alguns projetos, principalmente os que são automatizados após sua construção – como antigos museus de arte, seria interessante a aplicação de um protocolo sem fio.

Para tais aplicações, surgiu uma nova tecnologia, a *wireless*, capacitando dispositivos eletrônicos como PCs, *notebooks*, PDAs, telefones celulares, *modems*, impressoras e outros, se comunicarem a curta distância sem a utilização de cabos. Essa nova tecnologia é denominada *Bluetooth*, a qual vem ganhando suporte de importantes fabricantes como IBM, Ericson, Nokia, Toshiba, Microsoft, Intel e muitos outros. Essa tecnologia possibilita diferentes dispositivos de diferentes fabricantes se conectarem automaticamente formando uma rede denominada *scatternet*. Os tópicos a seguir darão uma visão geral sobre essa nova tecnologia.

6.1.1 Tecnologia

De acordo com Amory e Junior (2001), *bluetooth* é uma especificação aberta (*royalty-free*) de uma tecnologia padrão para comunicação sem fio ad hoc, de curto alcance e baixo custo, através de conexões de rádio. Por meio dessa especificação, os usuários poderão conectar uma ampla variedade de dispositivos fixos (PCs, impressoras, *mouse*, teclado, *scanners*, etc.) e móveis (*laptops*, PDAs, telefones celulares, etc.) de uma forma bastante simples, sem a necessidade de utilizar cabos de ligação. A idéia é permitir a interoperabilidade desses dispositivos de forma automática e sem que o usuário necessite se

preocupar com isso. O padrão *Bluetooth* visa facilitar as transmissões de voz e dados em tempo real, assegurar proteção contra interferência e a segurança dos dados transmitidos.

A idéia inicial do *Bluetooth* era basicamente eliminar a necessidade de cabos para estabelecer comunicação entre dispositivos. Contudo, com o andamento do projeto, ficou claro que as aplicações de uma tecnologia desse tipo eram ilimitadas. Alguns exemplos da aplicabilidade do *Bluetooth* são apresentados a seguir:

- O celular de uma pessoa pode saber automaticamente quando se encontra perto do *notebook* do mesmo dono, podendo assim enviar-lhe as mensagens de correio eletrônico recebidas da Internet sem que o ser humano precise se preocupar com isso;
- Um dispositivo *Bluetooth* funcionando como um identificador pessoal de um usuário pode se comunicar com outros dispositivos *Bluetooth* em sua residência. Após chegar a casa, a porta automaticamente se destrava para o usuário e as luzes são acesas;
- Mais uma vez, um dispositivo *Bluetooth* contendo informações pessoais de um usuário pode funcionar com uma carteira eletrônica de dinheiro. Ao se fazer compras, uma registradora desconta o valor da mercadoria adquirida.

Segundo Haartsen (2000), dispositivos *Bluetooth* operam na faixa ISM (*Industrial, Scientific, Medical*) centrada em 2,45 GHz, que era formalmente reservada para alguns grupos de usuários profissionais, mas que recentemente tem sido aberta mundialmente para uso comercial.

Os dispositivos *Bluetooth* comunicam-se entre si e formam uma rede denominada *piconet*, na qual podem existir até oito dispositivos interligados, sendo um deles o mestre (*master*) e os outros dispositivos escravos (*slaves*). Tipicamente, nas aplicações *Bluetooth*, várias *piconets* independentes e não-sincronizadas podem se sobrepor ou existir na mesma área. Neste caso, forma-se um sistema ad hoc disperso denominado *scatternet*, composto de múltiplas redes, cada uma contendo um número limitado de dispositivos. A figura 6.1 apresenta essas idéias.

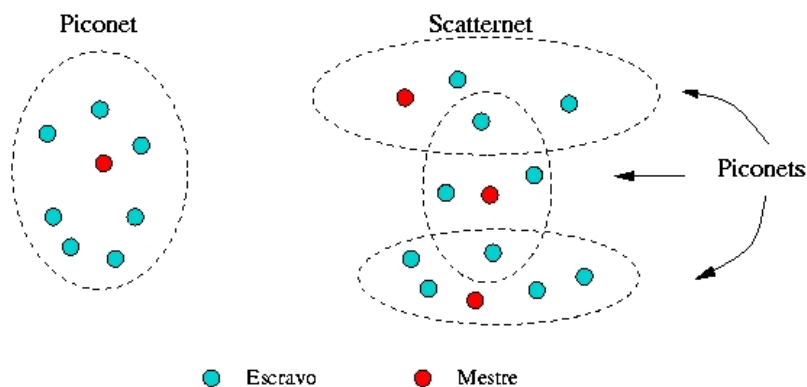


Figura 6.1 – Tipos de redes formadas entre dispositivos *Bluetooth*. Fonte: BLUETOOTH, 2005

6.1.2 Esquema de Acesso Múltiplo

Segundo Haartsen (2000), a comunicação entre os dispositivos *Bluetooth* é feita através do estabelecimento de um canal FH-CDMA (*Frequency Hopping - Code-Division Multiple Access*) onde, na média os sinais podem ser propagados sobre uma grande faixa de frequência, mas instantaneamente, somente uma pequena largura de banda é ocupada, evitando potenciais interferências na faixa ISM. Na tecnologia *Bluetooth* foram definidas 79 *hops* (portadoras) espaçadas em 1 MHz. Essa frequência gera uma razoável largura de banda e a melhor imunidade à interferência. Portanto, existem 79 frequências nas quais instantaneamente um dispositivo pode estar transmitindo. A sequência particular de frequências de um canal é estabelecida pelo dispositivo mestre da *piconet*, que é o responsável pelo controle do canal. Todos os outros dispositivos participantes da *piconet* são *slaves* e devem se sincronizar ao mestre.

6.1.3 Controle de acesso ao meio

O *Bluetooth* foi otimizado para permitir que um número elevado de comunicações não coordenadas ocorram dentro da mesma área. De modo diferente de outras soluções ad hoc, onde todos os dispositivos compartilham o mesmo canal, no *Bluetooth* existe um grande número de canais independentes, cada qual servindo somente um número limitado de participantes.

Um canal (FH *Bluetooth Channel*) está associado a uma *piconet* e é identificado pela sequência de frequências e pelo relógio do dispositivo mestre. Esse dispositivo controla o tráfego na *piconet* e também cuida do controle de acesso. Para evitar a colisão devido a múltiplas transmissões de dispositivos escravos, o dispositivo mestre utiliza a técnica de *polling*. Deste modo, somente o dispositivo indicado no slot mestre-para-escravo pode transmitir no *slot* escravo-para-mestre seguinte.

6.1.4 Estabelecendo Conexões

Para se criar uma rede *Bluetooth* ou para se adicionar componentes a uma *piconet*, os dispositivos devem ser identificados. Dispositivos podem ser dinamicamente conectados e desconectados de uma *piconet* a qualquer hora.

Quando um dispositivo deseja estabelecer uma conexão e não sabe quais são os outros dispositivos que estão em sua área de alcance e suas características, ele difunde mensagens do tipo *inquiry*. Ao receber uma mensagem desse tipo, um dispositivo deve retornar um pacote do tipo FHS (*Frequency Hopping-synchronization*) contendo além de seu identificador, informações para o sincronismo entre os dispositivos. Os dispositivos que respondem a uma mensagem de *inquiry* utilizam uma temporização aleatória para enviar a resposta. O objetivo é evitar possíveis colisões, quando mais de um dispositivo responder ao pedido.

Depois de coletar informações sobre os outros dispositivos, o dispositivo que deseja estabelecer a conexão pode utilizar uma mensagem do tipo *page* para realmente estabelecer uma conexão, isto é, uma mensagem do tipo *page* é somente utilizada por um dispositivo que deseja estabelecer uma conexão com algum outro dispositivo cujo identificador e informações de sincronismo são conhecidas.

Os dispositivos que estão ociosos podem permanecer num estado de *stanby* para economizar energia. Contudo, periodicamente eles devem "acordar" para verificar se existe algum outro dispositivo tentando se comunicar. Neste momento pode-se dizer que a unidade está em estado de *SCAN*.

6.1.5 Tipos de Links

Uma vez conectado a uma *piconet*, um dispositivo pode se comunicar através de dois tipos de *links*:

- *Synchronous Connection Oriented (SCO) link*;
- *Asynchronous Connectionless (ACL) link*.

É importante colocar que diferentes tipos de *link* podem ser aplicados entre diferentes pares de *master-slave* numa mesma *piconet* e o tipo de *link* pode mudar arbitrariamente durante uma seção. O tipo do *link* define quais os tipos de pacotes podem ser usados.

Um SCO é um *link* ponto-a-ponto entre o *master* e o *slave*. Esse *link* é tipicamente usado para a transmissão de voz.

Um *link* ACL faz uma conexão momentânea entre o *master* e qualquer *slave* de uma *piconet*. Esse *link* é tipicamente utilizado para a transmissão de dados.

6.2 Tecnologia Wi-Fi

A tecnologia Wi-Fi interliga computadores sem o uso de fio. Atualmente, é o sistema de conexão em rede que mais cresce no mundo. No Brasil, estima-se que menos de 3% dos usuários de banda larga - que são quase 3 milhões - usem conexão sem fio em casa.

Graças a essa taxa de adoção tão baixa, as empresas do setor apostam em forte crescimento nos próximos anos. A D-Link, líder no mercado wireless doméstico, aumentou em 329% o número de unidades vendidas no primeiro trimestre deste ano, em comparação com o mesmo período do ano passado. A LinkSys, braço "doméstico" da gigante Cisco, dobrou as vendas entre 2004 e o ano anterior.

Com preços em queda e configuração mais simples, a instalação de uma rede sem fio tem tudo para oferecer, além de acesso, serviços que poucos imaginam. É possível, por exemplo, colocar um adaptador de mídia na TV ou no home theater da sala, para que eles possam exibir vídeos e músicas guardados no PC, ou ainda usar uma webcam para monitorar o ambiente doméstico via Internet. No futuro, estimam os especialistas, haverá uma infinidade de aparelhos ligados entre si via rede - desde a torradeira até a máquina de lavar.

Um conceito muito importante e usado no mundo Wi-Fi é o 802.11, seguido da letra b, g ou a. Esse número refere-se a um padrão de transferência de dados, que permite a dois ou mais micros comunicarem-se entre si por ondas de rádio.

O padrão mais adotado no mundo atualmente é o 802.11b. Equipamentos com essa tecnologia transmitem dados a, no máximo, 11 Mbps (megabits por segundo). No mundo real, no entanto, o normal são transferências de até 3,5 Mbps. A vantagem é que os aparelhos 802.11b são os mais baratos hoje em dia.

Em empresas, adota-se o padrão 802.11a, criado juntamente com o "b". O "a" é muito mais rápido - até 54 Mbps -, mas tem alcance menor e sofre mais com paredes e outras obstruções. Por isso, é mais adotado em escritórios.

No final de 2003, surgiu o protocolo 802.11g, uma tentativa de combinar o melhor dos outros dois. Ele também é rápido - 54 Mbps - e compatível com aparelhos de

tecnologia "b" (mas não com padrão "a", que usa outra frequência de transmissão). Além disso, tem bom alcance e não perde tanto a força com paredes. Por isso, atualmente a melhor escolha para o usuário doméstico são equipamentos com a tecnologia 802.11g.

Definido-se isso, define-se agora o próximo termo: o roteador (*gateway*). Esse equipamento irá "inundar" o ambiente com ondas de rádio, permitindo que os micros conversem entre si. O roteador é ligado por um cabo ao modem que recebe a conexão da Internet - seja ela via telefone ou cabo.

Depois, cada micro que fará parte da rede precisa de um adaptador para entender o sinal do *gateway*. Esse equipamento pode ter dois formatos: padrão PCI ou USB. O PCI é uma placa que vai encaixada dentro do computador, ao lado do modem e da placa de vídeo, por exemplo. Para instalá-lo, é preciso abrir o gabinete e localizar um *slot* (encaixe) livre. Já o USB, embora um pouco mais caro, é infinitamente mais simples: basta espetar o adaptador na saída USB.

Feito isso, basta ligar o micro onde o roteador foi ligado e esperar o Windows reconhecer o equipamento. Em geral, o fabricante fornece um CD de instalação - basta executá-lo e ele faz o serviço. Se tudo der certo, em alguns minutos a rede sem fio estará pronta e operante.

6.2.1 Segurança

Na parte de segurança alguns fatores são importantes quando se trata de redes sem fio.

O primeiro é o alcance do roteador - em média, o sinal tem um raio de 50 metros, em todas as direções. Se a casa for grande ou a intenção for usar o notebook no jardim, talvez seja preciso comprar uma antena repetidora, que amplifica o sinal.

Além disso, é possível que o sinal sofra interferências. A tecnologia 802.11g (e a "b") opera na frequência de 2,4 GHz, usada por alguns telefones sem fio e pelos fornos microondas. Se a interferência for severa (em regiões com muitas empresas, por exemplo),

o jeito é comprar equipamentos de padrão 802.11a, que são mais caros e têm alcance menor.

E, para evitar problemas como invasões, os cuidados são os mesmos de uma rede fixa: usar senhas não-óbvias e ter sempre instalados um antivírus e um firewall. O antivírus evita que pragas virtuais invadam o sistema e enviem informações para fora. Já o firewall barra tentativas de invasão externas, igualmente perigosas. Alguns fabricantes já possuem aparelhos com firewall incorporado, o que ajuda muito na segurança da rede.

6.3 Tecnologia Wi-Max

A tecnologia Wi-fi funciona bem, mas somente em alcances relativamente curtos - até 100 metros em ambientes abertos e 50 metros em fechados. Por isso, para oferecer conectividade em escalas de quilômetros, empresas - e até cidades - têm adotado uma nova tecnologia: o WiMax. A sigla significa "Interconexão Mundial por Acesso em Microondas", e é fruto de um consórcio de 140 empresas de tecnologia, com a gigante dos chips Intel à frente.

Um ponto WiMax permite oferecer conexão em um raio de até 50 km, com velocidade máxima de 70 Mbps (Megabits por segundo) - isso em tese, porque na prática a topografia e os prédios de uma cidade grande podem interferir muito na transmissão. A desvantagem é que essa tecnologia só funciona se os equipamentos estiverem parados. Comunidades, vilas e até cidades inteiras poderiam ter conexão à Web sem os pesados custos envolvidos na instalação de cabos telefônicos ou de TV. A tecnologia ainda está em fase de certificação (padronização), que deve acontecer ao longo de 2005.

Já se tem alguns *cases* reais:

- Cidades como Los Angeles, Nova York, Boston, Seattle e Chengdu (China) estão fazendo testes com redes WiMax. No final do mês de abril deste ano, Brighton tornou-se a primeira cidade na Inglaterra a lançar uma rede Wi-Max, que cobre 90% de sua área urbana. O projeto foi fruto de

parceria entre a prefeitura, a Universidade de Sussex e a companhia local de telefonia. O objetivo era levar acesso à Web para sete escolas e três universidades na cidade, a custos menores do que com instalação de cabos ou tecnologia celular de terceira geração (3G).

- Nos EUA, algumas cidades estão com planos de implantar redes públicas em WiMax, mas enfrentam resistência das companhias telefônicas, que têm no acesso em banda larga uma boa fonte de lucros. Na Filadélfia, por exemplo, a prefeitura lançou um serviço de banda larga sem fio por US\$ 20 ao mês para os moradores de baixa renda, abaixo dos US\$ 30 cobrados no plano mais barato da Verizon, a operadora local.
- No Brasil, a experiência pioneira acontece em Sud Menucci, no interior de São Paulo. Em junho de 2003, a cidade, de apenas 7.500 habitantes, lançou um serviço de acesso gratuito em Wi-Fi (802.11b). Qualquer cidadão pode navegar na Web, bastando pedir uma senha para a prefeitura.
- No mês de abril, a Intel anunciou que Ouro Preto, em Minas Gerais, será base para o segundo projeto de rede WiMax no país (o primeiro acontece em Brasília). Cinco escolas públicas de ensino fundamental e médio são interligadas pelo sistema, além da Universidade Federal de Ouro Preto. Uma sub-rede conecta um telecentro, quatro secretarias de governo e uma associação de desenvolvimento comercial. O conteúdo oferecido é educacional.

7 CÂMERAS DE VÍDEO

A função principal de uma câmera é fixar o foco da imagem que foi capturada da lente óptica, e que através do CCD se transforma em sinais de vídeo e são processadas pelos componentes internos da câmera. Através de cabos, fibra óptica ou outros meios de transmissão os sinais de vídeo são transmitidos para o monitor.

Atualmente, já existe no mercado tanto câmeras preto e branco (P/B), que utilizam tecnologia do sistema EIA, como coloridas, que utilizam tecnologia do sistema NTSC.

Os tipos de sensores de imagem mais comuns das câmeras são o tube, o CCD e o CMOS.

Além disso, tem-se a classificação das câmeras em alta sensibilidade – alta resolução, e baixa sensibilidade – resolução regular.

7.1 Definições

EIA – *Eletronics Industry Association* – entidade americana que definiu o padrão de televisão utilizado nos EUA, Canadá e Japão, baseado no *scanning* entrelaçado com 252 linhas. Inicialmente conhecida como RMA ou RETMA.

NTSC – *National Television System Committee* – entidade americana que estabeleceu o padrão do sistema de televisão em uso nos Estados Unidos, Canadá, Japão e algumas partes da América do Sul. Neste sistema, é utilizada uma onda sub-portadora com frequência de 3,57945 MHz, cuja fase varia com a saturação instantânea da cor; no sistema NTSC tem-se 525 linhas por quadro e 59,94 campos por segundo.

7.2 Sensores CMOS x sensores CCD

Com poucas exceções as câmaras profissionais atuais utilizam primariamente os sensores CCD. Esse tipo de sensor mostrou-se bastante adequado para as aplicações profissionais e apresenta uma grande variedade. Os CCDs mais comuns são os de Quadro Cheio e o Entrelaçado. Esses dispositivos serviram bem para a categoria de câmaras profissionais devido às suas comprovadas características de desempenho. Apesar dos CCDs apresentarem excelente desempenho de imagens, eles exigem circuitos eletrônicos sofisticados e de alto consumo de energia para o seu funcionamento. Os circuitos também ocupam um considerável espaço no interior da câmara porque os CCDs não têm a capacidade de incorporar os circuitos de suporte ao sensor. O processo de fabricação utilizado nos CCDs não é compatível com o padrão de processamento do CMOS, o qual é utilizado atualmente na maioria dos componentes eletrônicos baseados no silício.

Como os CCDs são dispositivos de carga acoplada e de leitura por deslocamento da carga eletrônica da imagem de pixel a pixel, eles requerem consideráveis circuitos externos de sincronização que consomem espaço e energia. Mas por causa da complicada estrutura de leitura, o conjunto de recursos do dispositivo é muito limitado. O fato mais importante é que os CCDs são excelentes dispositivos de geração de imagens, mas não são muito flexíveis e carecem de alguns recursos desejáveis.

Os sensores CMOS são fabricados utilizando o processamento de silício CMOS padrão e por essa razão podem incorporar circuitos eletrônicos de suporte embutidos no chip. Alguns sensores CMOS incorporam até um conversor analógico-digital, o que reduz significativamente as exigências de espaço e de consumo de energia da câmara. Adicionalmente, os sensores CMOS têm uma propriedade exclusiva que simplifica as operações de tratamento de imagens; dentro de cada pixel, a carga eletrônica que é gerada a partir do contato da luz com o fotodiodo é convertida diretamente numa voltagem utilizável. Por essa razão, o processo de leitura é realizado através da utilização tradicional de transistores e de amplificadores. Isso permite características únicas como leitura direta da sub-amostragem on-chip e da região de interesse.

Os sensores CMOS, embora tenham características altamente desejáveis, também apresentam algumas propriedades que necessitam de uma atenção cuidadosa. Uma delas é o ruído-padrão fixado. Como os sensores CMOS utilizam amplificadores de voltagem dentro do pixel e, também, em outras seções do subsistema de leitura, nem todos os pixels responderão da mesma maneira aos sinais de luz e de escuridão. Isso acrescenta um padrão fixo à imagem; a boa nova aqui é a palavra "fixo". Desde que o padrão seja o mesmo para cada imagem, ele poderá ser removido com técnicas de processamento de imagens.

7.3 Câmeras Estudadas

As câmeras encontradas no mercado fazem um sistema de vigilância de vídeo multi-canais baseado em PC. Utiliza-se tecnologias avançadas de compressão de vídeo digitais para obtenção de alta qualidade de imagem e alto desempenho de vídeo. Pode-se ter um máximo de 16 câmeras conectadas e vistas ao vivo em uma tela de monitor local ou através de rede, em outros locais.

O vídeo pode ser gravado por programações específicas ou pela detecção de movimento – que é o mais usado.

7.4 Sistema *GeoVision*

O *Geovision* é um sistema de vigilância digital completo composto por uma placa que deve ser conectada ao microcomputador por meio de um *slot* PCI. Este sistema é fornecido em diversos modelos, de maneira a atender as diferentes situações, proporcionando assim um excelente custo benefício, não havendo a necessidade de se

investir em recursos que não serão utilizados. Há produtos que atendem desde o usuário doméstico a aplicações profissionais.

Sendo uma ótima opção onde se queira monitorar um determinado número de câmeras, seja em tela cheia ou no modo multiplexado (modo onde pode ser visualizada mais de uma câmera simultaneamente na tela), além desta característica o sistema também permite o monitoramento remoto das imagens bem como sua gravação no próprio HD. A gravação pode ser acionada através da função *motion detect* – detecção de movimento, ou por datas e horários programados.

7.4.1 Características

7.4.1.1 Modos de Visualização das Imagens:

- Tela cheia: É possível visualizar uma determinada câmera em tela cheia permitindo assim uma melhor riqueza quanto a detalhes.
- Multiplexado: Permite a visualização simultânea de diversas câmeras na tela em vários tamanhos e quantidades.
- Seqüencial: permite a visualização das câmeras uma a uma em tela cheia alternadamente.
- Visualização Remota: O sistema permite que as imagens sejam monitoradas remotamente seja através de rede local (LAN) e internet, suportando os seguintes protocolos TCP/IP, ISDN e ADSL.
- Resolução das imagens: Permite selecionar para cada câmera uma resolução específica a ser visualizada na tela, bem como o padrão de vídeo.

7.4.1.2 Modos de Gravação:

- Interativo: Permite o início ou término da gravação simultânea de todas as câmeras instaladas no sistema através de um simples clique do *mouse*
- Modo Programável: Permite selecionar de modo independente quais câmeras e em que horários a gravação deverá ser iniciada e finalizada.
- Modo Alarme: inicia a gravação assim que o sistema verificar uma variação na imagem, podendo ser ajustado o nível de sensibilidade.
- Remota: Permite realizar a gravação das imagens em qualquer outro local por meio de uma conexão remota.

7.4.1.3 Outras Características :

- Permite selecionar qual câmera deverá ser gravada, bem como sua definição e local.
- Permite controle de determinados modelos de câmeras e movimentadores via *software*.
- Permite a inclusão de senhas restringindo o acesso às configurações do sistema somente a pessoas autorizadas.

7.5 Multiplexador

O multiplexador é um equipamento utilizado para visualização de várias câmeras ao mesmo tempo. Normalmente ele pode ser SIMPLEX, DUPLEX ou TRIPLEX. Com o Simplex é possível apenas reproduzir. Já o Duplex permite a visualização das

câmeras enquanto se faz a gravação das imagens. E o Triplex tem as mesmas características do Duplex mais a possibilidade de assistir as imagens gravadas em tempo real.

Existem dois modos de exibição, em um deles são apresentadas todas as câmeras simultaneamente (divisão em até 16 quadros). No outro modo é apresentada uma câmera de cada vez (modo seqüenciado).

Muitos multiplexadores possuem a função zoom, onde é possível marcar um pequeno quadrado da imagem monitorada ou reproduzida para ser maximizado em tela cheia. Além de outras finalidades, é utilizado para identificação de pessoas ou objetos portados pelas mesmas. Alguns modelos fazem identificação de movimentação do local monitorado sem o uso de sensores, utilizando apenas a variação da imagem na tela.

7.6 Watchguard

O *watchguard* é um equipamento composto de uma placa para ser plugada no seu PC, onde podem ser conectadas através de quatro conectores RCA, até quatro câmeras P/B ou color.

Na tela do monitor do seu micro, é possível ver uma imagem em tela cheia; ou com a tela dividida; as quatro ao mesmo tempo. O equipamento permite gravar as imagens no HD, com ocupação de espaço a partir de 1Mbyte/hora de gravação, dependendo do nível de compactação, definição, e número de quadros por segundo.

O software possui a função *motion detect*, que permite através de demarcação com o *mouse* em uma área específica da imagem, monitorar e acionar um alarme e a gravação automaticamente quando ocorrer movimentação na região marcada, sem o uso de sensores, ou outro elemento qualquer.

Além do monitoramento local, é possível visualizar as imagens remotamente através da rede LAN, pela INTERNET, ou por conexão direta via linha telefônica. Em testes práticos, em uma linha com baixa qualidade, utilizando-se conexão fone-fone ou internet, com taxa de transmissão de 12kbps, obteve-se uma recepção de quatro quadros por

segundo. Este resultado pode em muito ser melhorado, utilizando-se linhas e modems de maior capacidade.

7.6.1 Aplicações

Recomenda-se o *Watchguard* como recurso para quem já possui um micro, para gravar as imagens em substituição ao videocassete, para eliminar ou obter os recursos de um multiplexador com custos menores, e como elemento de segurança aonde se deseja gravar imagens ou acionar alarmes no caso de intrusão.

É indispensável quando se deseja monitorar através de imagens via linha telefônica, internet ou rede LAN, um local remoto, como em rede de lojas e creches. Seu grande diferencial em relação aos outros equipamentos equivalentes no mercado, é o baixo custo, sem por isto deixar a desejar em suas características e confiabilidade.

7.7 Monitoração remota sem-fio via Internet ou Intranet

Uma boa opção que existe atualmente para uma monitoração remota ou transmissão de eventos em tempo real é a TRENDnet TV-IP100W. Ele é um servidor de câmera sem fio que transmite imagens pela Internet. Com a flexibilidade de conectividade em rede IEEE 802.11b e 10/100 Mbps, o TV-IP100W funciona como uma câmera de vídeo/vigilância, permitindo que você assista eventos ao vivo no seu *web browser* via Internet ou Intranet.

Este servidor de câmera Internet suporta *streaming* de vídeo com qualidade VGA, captura automática de imagem e notificação de eventos através de e-mail, que fazem dele a solução ideal para aplicações de *broadcasting* de vídeo via Internet.

7.7.1 Benefícios:

- Facilidade de Integração: Conecta a redes 10/100 Mbps ou wireless IEEE 802.11b 11 Mbps;
- Econômico: Servidor *web* embutido, não requer computador e *software* adicional;
- Flexível: Instale-o em rede local ou conecte-o à Internet para monitoração remota;
- Performance: Resolução de 640 x 480 *pixels* colorida com taxa de vídeo de até 20 fps;

7.7.2 Características:

- Permite acesso remoto a partir de *web browser* para visualização de imagens ao vivo;
- Suporta rede TCP/IP, *e-mail* SMTP, HTTP e outros protocolos relacionados à Internet;
- Suporta configuração da *web* com proteção por senha;
- Suporta tanto redes locais *Ethernet/Fast Ethernet* 10/100 Mbps quanto redes *wireless* IEEE 802.11b 11 Mbps;
- Poderoso *Software* Aplicativo *Windows IP View* para monitoração de múltiplas câmeras, captura de imagens e gravação de vídeo;
- Notificação via *E-mail* com imagens capturadas quando o sensor de entrada for ativado;
- Enorme leque de aplicações para monitoramento de residências, escritórios, bancos, hospitais, além de variada gama de monitoração pública e industrial.

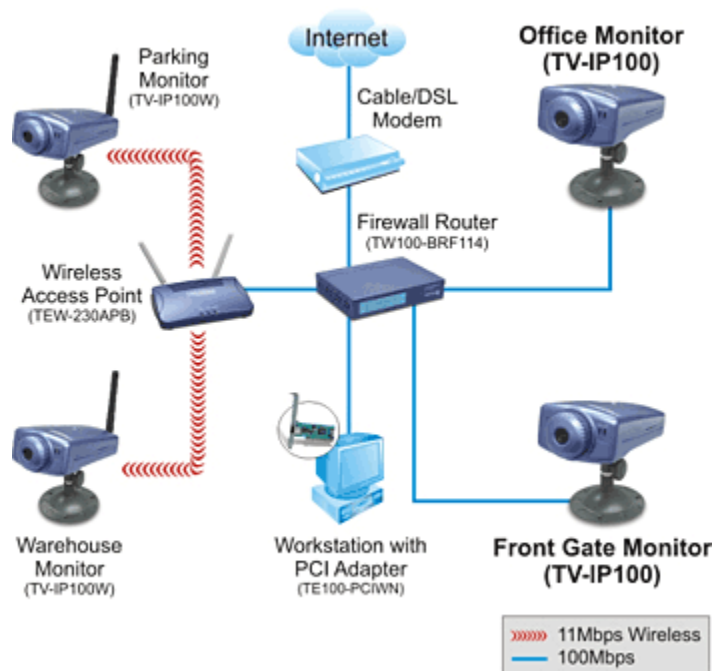


Figura 7.1 - Exemplo da rede trabalhando com a câmera.

Fonte: LINUXMALL, 2005

7.8 Disponibilizando Imagens na Internet

Para colocar uma câmera ao vivo na Internet, precisa-se de um micro, pelo menos uma *webcam*, uma conexão de Internet banda larga com um endereço IP público e um *software* especial. Não é possível usar conexão discada para colocar a câmera ao vivo (até dá, mas dever-se-ia que ficar conectado direto; se o usuário for viajar, por exemplo, torna-se inviável deixar o micro conectado direto na linha telefônica, por causa do altíssimo custo da conta telefônica depois). A questão de "endereço IP público" é a seguinte: o micro precisará ter um endereço IP que permita que qualquer outra máquina consiga acessá-la via Internet, justamente para se conseguir visualizar a câmera. A maioria dos serviços de Internet banda larga te dá um endereço IP público (endereço no formato 200.x.y.z). Entretanto, alguns serviços de banda larga – em especial os via rádio – não fornecem

endereço IP público. Este tipo de endereço começa com 192.168 ou então 10.0. Se a conexão com a Internet tiver um endereço deste tipo, o micro não pode ser acessado diretamente por outros micros da Internet, e, com isso, se fazem necessárias algumas configurações adicionais no programa (configuração de *proxy*, e provedor precisará ter um *proxy* configurado – a maioria tem).

O mais recomendado é o uso de *webcams* USB, pois são de simples instalação. Em geral os micros têm várias portas USB sem estarem sendo usadas. Além disso, cada porta USB permite a conexão de até 127 periféricos e mesmo que todas as portas USB do micro estejam sendo usadas, basta comprar um *hub* USB para expandir a quantidade de portas USB do micro.

Existem vários *softwares* para servidor de *webcam*. O *software* que recomenda-se aqui é o *webcamXP* e é um *shareware* válido por determinado tempo que pode ser baixado em <http://www.webcamxp.com>. Este programa suporta até 5 câmeras, significando que pode-se ter até 5 câmeras ao vivo na Internet ao mesmo tempo no micro. Após instalar este programa, só falta habilitar o micro como sendo um servidor de câmeras, bastando ir ao menu *web server* e habilitar a opção *enable http server*.

Com o servidor habilitado, pode-se ver as câmeras da casa ou empresa a partir de qualquer computador do mundo abrindo a página <http://a.b.c.d:8080>, onde a.b.c.d é o endereço IP do micro. Por exemplo, se o endereço IP do micro é 200.168.43.142, visualizam-se as câmeras no endereço <http://200.168.43.142:8080/>. Não sabendo-se qual é o endereço IP da máquina não tem problema: no menu *web server*, opção *HTTP settings* o programa dará essa informação.

Para colocar a câmera em um *site* na Internet, basta copiar o código que o programa te dá pronto no menu *advanced*, opção *generate HTML for your site*. Importante notar que o tráfego da câmera é redirecionado para o PC pessoal, isto é, os acessos serão feitos através do provedor de acesso e não através do servidor *web*. Isso significa que colocar uma câmera em um *site* não irá aumentar o tráfego gerado por ele (como os servidores de hospedagem cobram por tráfego, essa informação é importantíssima).

8 RECOMENDAÇÕES

A idéia do projeto é aplicável a automação predial ou residencial, mas também muito útil para ser aproveitada em empresas.

Citam-se alguns exemplos reais.

Em um supermercado onde o dono queira ter uma vigilância automática, 24 horas por dia, mas não tem muito capital para investir, tem-se uma solução possível.

Ele pode optar por colocar na entrada uma câmera de alta resolução, que identificará as pessoas perfeitamente. No resto do ambiente ele coloca câmeras de resolução mais baixa, que são bem mais baratas, e terão o papel de reconhecer a trajetória da pessoa.

Esse projeto também seria bem aplicado em museus e igrejas históricas. Nesse tipo de projeto, além dessa aplicação citada também se pode usufruir da câmera que utiliza a tecnologia *bluetooth*, para não carregar o ambiente.

Outro projeto interessante e aplicável seria o caso da Samarco, Mariana – MG. Neste, existe uma correia transportadora que transporta minérios. A correia transportadora não pode parar, porque a produção pára imediatamente. Para complicar, ela fica em um local de difícil acesso, onde os operadores tem certa dificuldade para chegar imediatamente.

Como solução foi feita a instalação de uma câmera monitorando essa correia transportadora. A câmera pode funcionar 24 horas ou ser acionada, por exemplo, pela própria correia transportadora quando esta estiver em alguma situação de risco. Na sala de operação, local de fácil acesso, fica instalado um supervísório. Com isso tem-se uma manutenção preventiva e, com certeza, diminuiram as paradas de produção.

Em um caso mais específico do trabalho, poder-se-ia ter em uma residência automações utilizando antenas para comunicação. A pessoa poderia ter uma antena no próprio carro e, por exemplo, no caminho de casa controlar a residência para que tome certas atitudes, como ligar a iluminação da entrada. Ou poderia, através das câmeras, fazer um passeio virtual pela residência e checar se está tudo certo para sua chegada. Portanto,

como foi relatado, as aplicações nessa área de segurança em automação são inúmeras; só dependem da criatividade do engenheiro que está projetando e do capital disponível para a implementação do projeto.

Para um projeto de automação predial completo, recomenda-se que seja implementado esse trabalho proposto juntamente com os projetos do Costa (2005), Meyer (2005) e Bueno (2005), que tratam de controle de demanda, bombeamento inteligente, controle de acesso e trancas automáticas.

9 CONSIDERAÇÕES FINAIS

Em qualquer trabalho de automação predial o fator econômico pode marcar o limite da sofisticação a atingir. Paralelamente, pode ocorrer desperdício quando não há adequação entre a tecnologia e o problema que se pretende resolver. A introdução de sistemas de automação predial visa trazer mais conforto ao usuário com significativa redução do consumo de energia e recursos naturais. Assim sendo, cada ambiente deve ser projetado com o intuito de promover uma convivência natural e pacífica entre o usuário e a tecnologia, sem imposição.

Através da domótica, está se propondo uma grande quebra de paradigma nos costumes da sociedade, onde pessoas que possuem dificuldades de se dedicarem aos seus lares poderão em um futuro breve controla-los remotamente através da internet.

Segundo a arquitetura do sistema proposto, além do computador Cliente, tem-se a necessidade de um computador Servidor, que estaria localizado diretamente dentro da residência, cuja responsabilidade principal é servir de *gateway* entre o navegador *Web* e as aplicações domésticas encontradas na residência.

Na área de *hardware*, o protocolo de comunicação escolhido foi o CAN, pois o mesmo é utilizado em maior número de aplicações, amplamente usado no ramo de automação, possui robustez e controle de erros. No caso da preferência por uma tecnologia sem fio, foi estudada a solução *Bluetooth*.

Percebe-se que mecanismos de segurança são prioritários no desenvolvimento de aplicações que envolvem domótica, garantindo neste caso a segurança do sistema de automação predial.

A domótica é uma área que está apenas recentemente começando a ser explorada, ao contrário de outras áreas. Sendo assim é importante o desenvolvimento de pesquisa e trabalhos científicos nesta área, garantindo neste caso que a domótica progrida e se popularize.

Pode-se ressaltar uma novidade que estará surgindo, em um futuro não muito distante. Essa novidade é o *streaming* de vídeo através do celular. Com isso, pode-se

dizer que em pouco tempo as pessoas poderão monitorar as residências ou escritórios através do próprio celular, eliminando a necessidade de um computador cliente.

REFERÊNCIA BIBLIOGRÁFICA

AMORY, Alexandre e JUNIOR, Juracy Petrini. **Sistema Integrado e Multiplataforma para Controle Remoto de Residências**. Dissertação (Mestrado em Engenharia) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2001, 166f

MARIOTONI, Carlos Alberto e JUNIOR, Edivaldo P. de Andrade. **Descrição de Sistemas de Automação Predial Baseados em Protocolos PLC Utilizados em Edifícios de Pequeno Porte em Residências**, 2001. 8f

BOLZANI, Caio Augustus Morais. **Desenvolvimento de um Simulador de Controle de Dispositivos Residenciais Inteligentes: uma introdução aos sistemas domóticos**. Dissertação (Mestrado em Engenharia) – Universidade de São Paulo, São Paulo, 2004, 130f.

NEVES, Raissa Pereira Alves de Azevedo. **Espaços Arquitetônicos de Alta Tecnologia**. Dissertação (Mestrado em Arquitetura e Urbanismo) – Universidade de São Paulo, São Paulo, 2002. 167f

BLUETOOTH. Disponível em: <http://www.bluetooth.com.br/>. Acesso em junho de 2005.

HAARTSEN, Jaap; **The Bluetooth Radio System, IEEE Personal Communication..** pp. 28-36. 2000.

HAARTSEN, J.; NAGHSHINEH, M.; INOUE, J.; **Bluetooth: Vision, Goals, and Architecture, Mobile Computing and Communications Review**. Volume 1, Number 2.

MANGER, Daniela Morais. **Conceitos de um Edifício Inteligente**. Trabalho (PET CIVIL). Universidade Federal de Ouro Preto, Ouro Preto, 2004.

BOLZANI, Caio Augustus Moraes. **Residenciais Inteligentes**. São Paulo, 2004, Editora Física, 1ª edição.

FOUCAUT, Michel. **As palavras e as Coisas: uma arqueologia das ciências humanas**. São Paulo: Martins Fontes, 1990.

CASTRO, Vicente Gonzáles: **“Teoría y Práctica de los Medios de Enseñanza”** – Editorial pueblo e Educación, C. de La Habana, 1986.

RIBEIRO, Leila Beatriz. **A Incorporação do Conceito de Sistema na Ciência da Informação**, Dissertação (Mestrado), Universidade Federal do Rio de Janeiro, Rio de Janeiro, 1993.

ALVES, Luiz Fernando Rísoli. **Higiene Escolar: Una metodología basada en un abordaje pedagógico y sistémico para mejorar las condiciones físicas de los salones de clase de la UFOP**. Dissertação (Doutorado). Havana, 2002.

COSTA, Bruno César da. **Controle de Nível em Sistemas de Automação Predial**. Trabalho (Monografia para graduação em Engenharia de Controle e Automação). Universidade Federal de Ouro Preto, Ouro Preto. 2005.

MEYER, Gabriel Ladeira. **Controle de Irrigação em Sistemas de Automação Predial**. Trabalho (Monografia para graduação em Engenharia de Controle e Automação). Universidade Federal de Ouro Preto, Ouro Preto. 2005.

BUENO, Kássio Damaso. **Controle de Dispositivos utilizados em Sistemas de Automação Predial via Web**. Trabalho (Monografia para graduação em Engenharia de Controle e Automação). Universidade Federal de Ouro Preto, Ouro Preto. 2005.

www.aureside.org.br, acesso em fevereiro 2005

www.linuxmall.com.br, acesso em 15 de julho de 2005

www.webcamxp.com, acesso em 15 de julho de 2005.