FERNANDO EIJI MUNAKATA
HELCIO YUKIO ICHIKAWA

nota final
7,6 (sete e seis)

MODELAGEM E VERIFICAÇÃO DE SISTEMAS DE AUTOMAÇÃO PARA SEGURANÇA RESIDENCIAL

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título em Engenharia.

São Paulo
2005

FERNANDO EIJI MUNAKATA
HELCIO YUKIO ICHIKAWA

MODELAGEM E VERIFICAÇÃO DE SISTEMAS DE AUTOMAÇÃO PARA SEGURANÇA RESIDENCIAL

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título em Engenharia.

Curso:
Engenharia Mecatrônica

Orientador: Prof. Doutor Paulo Eigi Miyagi

São Paulo
2005

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DA ENGENHARIA MECÂNICA/NAVAL DA ESCOLA POLITÉCNICA EPMN - USP

1600847

Munakata, Fernando Eiji. Ichikawa, Helcio Yukio

Modelagem e Verificação de Sistemas de Segurança para Automação Residencial, São Paulo, 2005.

80p.

Monografia (Graduação) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

1. Automação Residencial 2. Casa Inteligente 3. Sistema de Segurança 4. Rede de Petri 5. Metodologia de Modelagem

Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

Dedico este trabalho
aos nossos pais
que têm
sido a grande razão e
incentivo de nosso
aperfeiçoamento técnico.

AGRADECIMENTOS

Ao nosso orientador Prof. Dr. Paulo Eigi Miyagi, pelas diretrizes seguras, orientação, supervisão, confiança, paciência e oportunidade que concedeu-nos para o desenvolvimento deste trabalho e por todo o apoio prestado durante este ano.

Ao M.Eng. Fabrício Junqueira, pela colaboração, apoio, sugestões e discussões levantadas ao longo do período de trabalho as quais foram fundamentais na elaboração e consolidação do trabalho.

Ao pessoal da Associação Brasileria de Automação Residencial, pela colaboração para a realização deste trabalho.

Aos nossos professores do curso de Engenharia Mecatrônica da EPUSP, pelos conhecimentos adquiridos ao longo de todo o curso.

A todos nossos amigos e familiares, pela ajuda e apoio.

A todos os que direta ou indiretamente contribuíram para a realização deste trabalho.

SUMÁRIO

APÊNDICE I **I**

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

SED	Sistemas a Eventos Discretos
RI	Residências Inteligentes
ISDN	Integrated Services Digital Networking
MFG	Mark Flow Graph
PFS	Production Flow Schema
CFTV	Circuito Fechado de Televisão

RESUMO

Dentro do conceito de automação residencial e casas inteligentes, este trabalho visa desenvolver uma modelagem de sistema de automação detalhando os procedimentos específicos para a parte dê segurança residencial.

A abordagem considerada para este propósito baseia-se na utilização da teoria dos sistemas a eventos discretos através da aplicação de técnicas derivadas de rede de Petri.

Neste contexto, o trabalho aplica um procedimento sistemático para a modelagem de um sistema de segurança residencial integrado a outros sistemas, atuando sob a estrutura de um controle centralizado.

O modelo resultante do sistema de segurança residencial é analisado e verificado através de técnicas e ferramentas de simulações, confirmando a efetividade da metodologia considerada.

Palavras-chave: Automação residencial, casa inteligente, sistema de segurança, rede de Petri, metodologia de modelagem.

ABSTRACT

Considering the home automation and smart home concept, this work aims to develop an automation system model detailing the specific procedure related to home security.

The approach is based on the use of discrete event system theory and techniques derived from Petri net.

In this context, this work applies a systematic procedure to model a home security system that is integrated to other home systems but working with a centralized control structure.

The resulting model of a home security system is analyzed and verified through simulation tools and techniques that confirm the effectiveness of the considered methodology.

Keywords: *Home automation, smart home, security system, Petri net, modeling methodology.*

CAPÍTULO 1

INTRODUÇÃO

Neste capítulo, são apresentados as motivações, justificativas e objetivos do desenvolvimento deste trabalho.

1.1. Motivações e Justificativa

A percepção da realidade sócio-econômica e tecnológica mundial tem tornado a preocupação com a segurança pessoal e patrimonial um fator crítico na sociedade atual. Especificamente na área residencial, existe necessidade da utilização de sistemas voltados a atender demandas referentes à segurança associado aos níveis crescentes de conforto e minimização de custos [Aureside, 2005].

Com as inovações tecnológicas, surgiram os conceitos de condomínios e residências inteligentes que procuram automatizar e otimizar os processos, recursos e serviços destas instalações através de integração de sistemas e um controle central. Desta maneira, ao se projetar um sistema residencial deve-se considerar sua integração a outros sistemas [Aureside, 2005].

Neste contexto, um sistema de segurança residencial deve possibilitar o monitoramento e qualquer acontecimento, evento ou procedimento que o usuário desejar, através de recursos da automação residencial, que garanta conforto, alta confiabilidade e redução de custos [Future House, 2005].

Os dados estatísticos mostram que a incidência de furtos a condomínios residenciais e comerciais é crescente nas grandes cidades. Muitos desses edifícios já dispunham de equipamentos e recursos para proteção física e, mesmo assim, se mostraram vulneráveis à ação de intrusos. A análise de episódios recentes indica que a imprudência dos funcionários e a utilização indevida dos equipamentos de segurança são os principais fatores que resultaram nos problemas de segurança [Aureside, 2005].

A implantação de sistemas de automação residencial já têm sido conduzida a alguns anos. Entretanto, ainda são poucas as técnicas que tratam de maneira adequada a integração efetiva de sistemas, não explorando assim todo o potencial da interação destes sistemas em relação à eficiência e segurança global.

Desta maneira, observa-se a necessidade de estudar novas abordagens. Em particular, verifica-se que ainda não existem procedimentos para a implementação de sistemas mecatrônicos integrados as políticas de gestão da automação residencial. Nesse contexto, uma das propostas que tem demonstrado sua eficiência como ferramenta de modelagem e análise de sistemas de controle é o conceito de sistemas a eventos discretos (SEDs) e da rede de Petri. Estes conceitos e teorias foram desenvolvidas de forma genérica, e em aplicações específicas são definidas diferentes interpretações. No caso da técnica do PFS/MFG (Production Flow Schema/Mark Flow Graph) que é uma interpretação da rede de Petri para a área de sistemas produtivos, destaca-se sua aplicabilidade a plantas de diversos portes. Esta técnica de modelagem para fins de planejamento e controle apresenta as características de flexibilidade e integração exigidas na área de automação residencial e representam uma potencial solução para a descrição e análise da integração dos sistemas envolvidos.

1.2. Objetivos

Dentro do contexto de casas inteligentes, este trabalho visa aplicar uma metodologia genérica de modelagem de sistemas de automação e detalhar os procedimentos específicos para a parte de segurança residencial. A abordagem considerada para este propósito baseia-se no conceito de sistemas a eventos discretos (SEDs) e técnicas derivadas de rede de Petri.

CAPÍTULO 2

RESIDÊNCIAS INTELIGENTES E SISTEMAS DE SEGURANÇA

2.1. Residências Inteligentes

Cada vez mais, novas tecnologias são disponibilizadas e desenvolvidas para os locais de trabalho, lazer e residência. Assim, mudanças conceituais na arquitetura, projeto das instalações e na própria utilização das residências estão transformando estes ambientes, constituindo-se em um tema de estudo amplo e multi-disciplinar que está relacionado com o conceito de "residência inteligente".

Cronologicamente, as residências inteligentes surgem depois dos seus similares nas áreas industriais e comerciais. Os chamados "prédios inteligentes" representam um produto que é o resultado da fusão de vários campos envolvidos no projeto e construção de edifícios, alguns dos quais haviam sido considerados no passado como essencialmente distintos e sem interseção como são a arquitetura interior e exterior, as tecnologias da computação e as telecomunicações, a ergonomia, os fatores humanos, os processos construtivos e as tecnologias de suporte e operação de edifícios em geral: aquecimento, ventilação e ar condicionado (HVAC), segurança, transporte e todas as tecnologias (construção civil, mecânica, elétrica e mecatrônica) envolvidas [Finley, 1991]. Apesar da natural diversidade entre estes sistemas automatizados, a automação residencial tem algumas características em comum e peculiaridades quando comparadas aos requisitos da automação comercial e industrial.

O interesse por este tipo de residência é justificado, quando se considera o custo relativamente baixo de projeto, de programação e de circuitos e cabos eletro-eletrônicos que vão de 2% a 3% do valor do imóvel face às vantagens operacionais oferecidas. O que pesa mais é o preço dos dispositivos e equipamentos eletrônicos necessários mas muitos empreendimentos já são entregues com automação mínima e cabeamento estruturado [Aureside, 2005].

Por outro lado, alguns equipamentos visando mais eficiência de alguma operação são instalados, como que aleatoriamente, impulsionados pela onda mercadológica do

momento e acabam resolvendo problemas localizados, mas sem nenhuma integração efetiva com outros equipamentos. Isto acaba resultando em frustrações para os usuários da automação, que acabam convivendo com sistemas autônomos e muitas vezes de difícil operacionalidade.

Cada nova tecnologia traz acoplado um novo vocabulário. Quando o assunto é residência inteligente, não é diferente: casa automática, casa inteligente, automação residencial, *retrofitting* de residência, domótica, etc. Como qualquer novidade, a automação residencial inicialmente foi percebida como um símbolo de status e modernidade. No momento seguinte, o conforto e a conveniência por eles proporcionados passam a ser decisivos. E posteriormente, podem tornar-se uma necessidade vital e um fator de economia [Bolzani, 2004].

Na automação residencial, em última instância, vale ainda o estilo de vida e preferências de quem vai residir no local. Por isso as soluções são muito pessoais e dirigidas; por exemplo, alguns clientes atribuem excessiva ênfase aos sistemas de segurança quando residem numa casa isolada, mas estes mesmos clientes ao optarem por num condomínio fechado podem abrir mão de alguns itens de segurança e, com o mesmo gasto, sofisticar seu home theater. Se um sistema eletrônico instalado em um ambiente não oferece o devido conforto ao usuário, em semanas ele vai ser desligado e deixado de lado. O usuário em geral tem resistência para assimilar novas senhas, funções complexas, interfaces não amigáveis, etc. Os equipamentos deveriam unificar os controles e processos tornando as interfaces mais simples. A casa automática deve ajudar nas tarefas diárias que tomam muito tempo ou evitar tarefas triviais tais como fechar as janelas quando se detecta chuva. A automação vai de fato ajudar o usuário, quando as soluções estiverem de acordo com o tipo de vida, os gostos pessoais e os recursos disponíveis [Bolzani, 2004].

2.1.1. Objetivos e características

Segundo Bolzani [2004], os usuários (proprietários/moradores) estão se tornando mais conscientes dos benefícios da automação residencial. Estes benefícios geram demanda para que os construtores incluam a automação residencial em suas novas construções e

ao mesmo tempo ainda ofereçam serviços da readequação (retrofitting) para residências já existentes. Alguns dos objetivos principais de automação residencial são:

- assegurar a satisfação das pessoas que moram dentro dele (segurança, eficácia e conforto, conveniência);
- racionalizar os custos (controle de energia, controle dos serviços de manutenção, etc);
- racionalizar a recepção e transmissão de informação, atuando como um recurso base para o gerenciamento das atividades internas e externas (interatividade);
- garantir a confiabilidade dos sistemas introduzidos.

Estes objetivos tentam ser alcançado nas residências de hoje através da introdução de automação em níveis e áreas distintas e com equipamentos diversos [Kroner, 1997]. O impacto das redes de comunicação domésticas e, por conseqüência, a da automação residencial, estão baseadas no fato de permitir a comunicação entre estes dispositivos e controlá-los através de um gerenciador central.

A idéia de uma plataforma de infra-estrutura comum tem o intuito de estabelecer um padrão mínimo de comunicações para as instalações [Bolzani, 2004]. Deste modo, os profissionais envolvidos na construção de um ambiente inteligente, os usuários e os fornecedores teriam como referencial a existência dessa solução comum. A Figura 2.1 exemplifica como as partes de uma rede de comunicação doméstica trabalham conjuntas. No centro, o integrador de sistemas residenciais é o responsável pela harmonia e interoperabilidade de todo o conjunto.

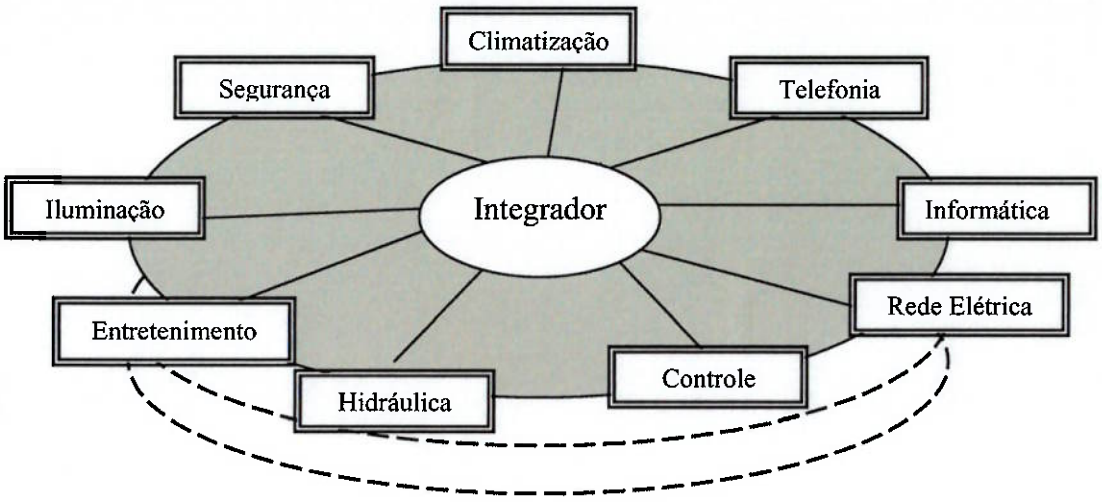


Figura 2.1 – Conceito de automação residencial

O principal fator a ser considerado na concepção de um projeto deste tipo é o planejamento do sistema de informação. Através da perfeita estimativa de como ele deve operar pode-se caracterizar os seguintes pontos: a integração, a interoperabilidade, a engenharia e a infra-estrutura inteligente [Bolzani, 2004].

A compatibilidade entre as partes deve ser assegurada, uma vez que a implantação poderá ser realizada em etapas e a integração somente estará garantida se as partes forem compatíveis entre si. Outro aspecto importante é a possibilidade de falhas, o que pode inviabilizar o funcionamento do sistema devido à arquitetura distribuída [Bolzani, 2004].

A implementação de um ambiente inteligente [Bolzani, 2004] pressupõe o planejamento de tarefas que até hoje não se observaram em construções residenciais, como:

- a organização dos sistemas de informática;
- os sistemas de gerenciamento da residência;
- a configuração das redes interna e externa de comunicações;
- a integração dos novos serviços de valor agregado;
- adaptação da rede aos vários moradores;
- a conexão aos serviços públicos de telecomunicações;

- máxima flexibilidade nas mudanças;
- organização do espaço interno e externo, com a introdução de novos equipamentos e novos dispositivos.

Como acontece no cotidiano, o fator econômico pode limitar o grau de sofisticação a atingir. Por outro lado, pode ocorrer desperdício de recursos quando não há adequação entre a tecnologia e o problema que se pretende resolver. Nos Estados Unidos, acredita-se que o investimento em sistemas de automação residencial corresponda em média a 10% do custo total da obra, com um retorno em médio prazo na forma de racionalização dos serviços de manutenção e economia nos gastos com energia, água e gás na ordem de 30%. Deste modo, o custo do sistema não é o principal problema, mas sim a incerteza quanto ao retorno da comodidade. Daí a necessidade de se projetá-lo como um todo, com atenção às funcionalidades computacionais. Assim, um simulador de dispositivos em uma residência inteligente é de grande valia pois permite avaliar o impacto das instalações de novos equipamentos e *softwares* [Bolzani, 2004].

Um sistema de gerenciamento efetua o controle e a coordenação dos diversos serviços. Nesta forma de organização da casa inteligente tem-se vantagens consideráveis para enfrentar uma situação muito diferente dos tempos em que os baixos custos e alta disponibilidade da energia permitiam uma atividade descuidada em relação ao consumo [Neto, 1994].

2.1.2. Integração de sistemas em residências inteligentes

Atualmente, pode-se definir até três níveis de interação no contexto da automação residencial [Aureside, 2005]:

- sistemas autônomos;
- integração de sistemas;
- residência inteligente.

No nível de sistemas autônomos pode-se ligar ou desligar um subsistema ou um dispositivo específico de acordo com um ajuste pré-definido. Porém, neste esquema,

cada dispositivo ou subsistema é tratado independentemente, sem que os dispositivos tenham relação um com o outro.

No nível de integração de sistemas tem-se múltiplos subsistemas integrados a um único controlador. A limitação deste sistema está em que cada subsistema deve ainda funcionar unicamente na forma a qual foi concebida pelo seu fabricante. Esta forma de integração permite uma ampla gama de benefícios ao usuário e garante eficiência no aproveitamento dos recursos utilizados.

No nível de residência inteligente os sub-sistemas são personalizados para atender às necessidades do usuário. O integrador de sistemas em conjunto com o usuário delinea instruções específicas para modificar o uso do ambiente. Assim, o sistema de automação torna-se um gerenciador ao invés de apenas um controlador remoto. Os sistemas de automação dependem da comunicação de mão-dupla e realimentação do estado de todos os subsistemas para um desempenho adequado.

Para tomar vantagem das novas tecnologias, os usuários têm uma expectativa maior quanto aos construtores fazerem as coisas de modo diferente do que antes faziam. Os construtores, de forma a participar deste lucrativo e novo mercado, precisam educar a si próprios e treinar ou contratar indivíduos para atuar como integradores e instaladores de sistemas de automação. A comunicação entre o construtor e/ou integrador e instaladores com os usuários é a chave para o sucesso. Um "bom" projeto de automação residencial resulta numa interface amigável para o usuário final, que dele poderá obter variados benefícios [Aureside, 2005].

2.2. Sistemas de segurança

Ao se citar vigilância eletrônica muitos ainda têm a idéia de um sistema de alta tecnologia voltado a espionar pessoas, mas os circuitos fechados de TV (CFTV) podem não só acrescentar segurança às residências, mas também conveniência [Bolzani, 2004].

De todos os sistemas domóticos, o de segurança é um dos mais procurados pelos usuários atualmente. Para estes sistemas é imprescindível criar soluções que sejam não somente compatíveis, mas também complementares com outros sistemas residenciais. O

sistema de segurança deve cumprir fundamentalmente os seguintes pontos considerados básicos [Bolzani, 2004]:

- prevenção ou dissuasão: criação de barreiras físicas ou virtuais, dispersando, dificultando ou ainda impedindo o propósito de intrusão ou ataque;
- detecção e alarmes: capacidade de se receber informações de sensores, entender seus estados e acionar atuadores;
- reconhecimento ou identificação: são mecanismos que possibilitam ao sistema diferenciar o usuário do não-usuário, e acionar os mecanismos de acordo;
- retardo: tempo em que o sistema analisa as condições dos sensores e câmeras e verifica a possibilidade de falsos alarmes ou espera por uma ordem do usuário;
- reação: efetivo disparo de atividades programadas a fim de retardar ou mesmo cancelar o processo de intrusão e emitir aviso.

Para que todos estes pontos sejam observados de forma eficaz é fundamental que o fluxo de informações seja tratado de maneira adequada, com eficácia e confiabilidade, estabelecendo um meio rápido e seguro de transmissão entre os diversos sensores e atuadores e a central de segurança da residência.

Nesta central, existem dois cenários básicos com que o sistema deve lidar: quando o usuário está em casa e quando não está. Deve ser capaz de prever várias situações de ataque e reagir com o propósito de nunca deixar o usuário em posição de risco eventualmente sinalizando ou acionando rotas de fuga, por exemplo. No caso da ausência de pessoas no local, o sistema deve estar apto a informar o usuário remotamente através de mensagens de alerta via rede de comunicação pública ou outro sistema de conexão com a polícia ou uma agência particular. Neste sentido, é de grande valia a apresentação visual e remota, de gráficos que indicam a situação, em planta, das partes afetadas, bem como as imagens das câmeras de vigilância. Finalmente, ele deve atuar em conjunto com os outros sistemas que controlam os demais serviços residenciais, tanto para receber informações como para sugerir ações (por exemplo, controlando o acionamento de luzes, trava de portas, etc) [Bolzani, 2004].

Os sistemas de segurança que são empregados na proteção de espaços e edificações, controlados através de uma central, podem ser divididos basicamente nos seguintes subsistemas:

- vigilância com circuito fechado de televisão (CFTV);
- controle e automação de acesso;
- detecção perimetral;
- sensoriamento interno e externo
- iluminação;
- redes de comunicação;
- alarme.

A seguir, apresenta-se mais detalhes sobre estes sub-sistemas.

2.2.1. Sub-sistema de vigilância com CFTV

Os componentes básicos de um sistema de vigilância são as câmeras e os monitores. Existem câmeras do tamanho de uma caixa de fósforos e outras maiores, de uso em ambientes especiais. Algumas câmeras são dotadas de detector de movimento. Elas podem inclusive emitir um som quando alguém se aproxima ou acionar a gravação da imagem em um *hard disk* de um computador se o sistema for digital [Bolzani, 2004].

As câmeras de CFTV, normalmente, são constituídas de um sensor de imagem *Charge Couple Device* (CCD) que é um circuito integrado com elementos fotossensitivos. Com a redução do tamanho dos sensores e da eletrônica na montagem dos equipamentos, obteve-se uma redução substancial nas dimensões físicas externas, satisfazendo as exigências dos arquitetos com relação à estética destes equipamentos para uso em residências. E ainda possível mudar o canal da TV passando a monitorar a imagem do CFTV sempre que alguém toca a campainha da casa ou quando um sensor de presença detecta algum movimento estranho [Bolzani, 2004].

Dentre as partes que compõem o CFTV, destacam-se:

- sequenciador: permite um sequenciamento na visualização das imagens de diferentes câmeras;
- multiplexador: permite a visualização de imagens de várias câmeras ao mesmo tempo em uma mesma tela;
- dome: caixa de proteção plástica em forma de domo e que impede a identificação da posição da câmera.

Cada sistema utiliza ainda diferentes componentes em sua configuração, mas todos possuem a estrutura da Figura 2.2:

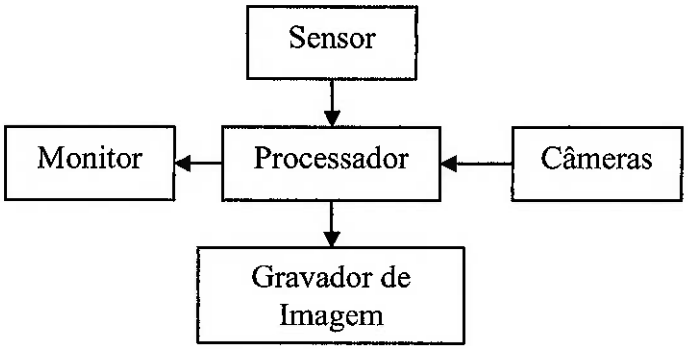


Figura 2.2 – Esquema de um sistema CFTV

A possibilidade de verificar as imagens do CFTV a partir de um local remoto é também um recurso útil. Alguns utilizam alguma rede de comunicação para transmitir as imagens de videocâmeras distribuídas pela casa [Bolzani, 2004]. A Figura 2.3 mostra alguns exemplos de dispositivos de um sistema CFTV.

Figura 2.3 – Dispositivos de um sistema CFTV

2.2.2. Sub-sistema de controle e automação de acesso

O sistema de acesso tem como objetivo principal efetuar o controle de pessoas (moradores, empregados e visitantes) e veículos dentro dos limites da residência. Já a automação do acesso permite a identificação prévia do visitante através de sensores e que possibilita efetuar determinadas ações e controlar o acesso a certos serviços de acordo com a programação desejada pelo usuário. Chaves eletrônicas, impressões digitais, reconhecimento de voz, leitura de íris ou mesmo de cartão magnético estão sendo desenvolvidos e alguns já são utilizados no ambiente residencial para a identificação e classificação dos usuários [Bolzani, 2004].

Em um sistema automatizado, cada morador da casa possui sua própria chave eletrônica que pode abrir as portas da residência sem a necessidade de se carregar várias chaves. Alguns modelos possuem um código interno único e são extremamente difíceis de serem copiadas; por esse motivo, são seguras e individuais, permitindo, por exemplo, que apenas o dono da casa tenha trânsito livre, e visitantes tenham acesso apenas aos seus quartos e os empregados possam abrir somente a porta de serviço dentro de certos horários. Se integrada a outros serviços, a chave eletrônica, pode ainda servir para desarmar o sistema de alarme ou acionar um tipo pessoal de iluminação, acionando

parcialmente as lâmpadas da sala, ligando a TV, e reproduzindo uma saudação personalizada. Caso o sistema não reconheça a pessoa pode-se acionar o sistema de CFTV e/ou utilizar um discador automático para avisar o morador. Se alguém tentar desligar ou danificar algum sistema ou parte importante deste, o sistema de alarmes deve ser acionado avisando o usuário ou a empresa de segurança contratada. Todos os eventos são registrados e armazenados numa central de controle de acessos e numa central de segurança [Bolzani, 2004].

As unidades leitoras (leitoras de cartão, identificação por radiofrequência, etc.) devem ser associadas a dispositivos eletromecânicos como catracas, fechaduras, etc. que efetuam o bloqueio físico das pessoas. Devem ser previstos também alarmes associados a eventos como portas deixadas abertas inadvertidamente [Bolzani, 2004].

De acordo com o projeto, "Delta Smart House", elaborado por estudantes da Universidade de Duke, o controle e automação de acesso devem ter as seguintes características:

- impenetrável;
- seletivo: apenas usuários com permissão terão acesso a residência;
- conveniente: usuários não têm necessidade de carregar nenhum tipo de dispositivo para ter acesso à residência;
- moderno: utilizar tecnologia de ultima geração;
- expansível: permitir a possibilidade de tratar um grande número de usuários no banco de dados;

Sabe-se que estas características são consideradas ideais e que não é possível cumprir todos os requisitos apresentados, uma vez que algumas características são contraditórias entre si.

Apresenta-se a seguir alguns dispositivos utilizados no sistema de controle de acesso:

Leitores biométricos

Biometria é definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um individuo. Elas incluem impressões digitais, voz, retina, íris, reconhecimento de face, imagem térmica, análise de assinatura, palma da mão e outras técnicas. Elas são de grande interesse em áreas onde é importante verificar a real identidade de um individuo. Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entretanto recentemente verifica-se sua utilização em uma grande e crescente área de situações em utilizações publicas no nosso dia a dia. Como as características analisadas pelos dispositivos são únicas e estão no corpo, as possibilidades de fraudes são menores [Amado, 2005].

Os leitores biométricos tornam mais simples o controle de acesso, sem a necessidade de chaves, cartões e senhas, e ainda aumentam a confiabilidade da segurança [Paradox, 2005].

Cartão de proximidade

O cartão de proximidade é, atualmente, largamente utilizado em prédios comerciais [Cdiport, 2005].

O sistema Hitag, foi o primeiro sistema apresentado pela Philips como resposta ao crescente interesse dos sistemas de controle de acessos, cada vez mais práticos e seguros. Este sistema funciona através RF (radio frequência), de modo que dentro de uma distância específica, seja possível a leitura e validação de um cartão [Oliveira, H.; Oliveira, T., 2004].

Existem hoje outras tecnologias e diversos fabricantes no mercado, assim, dependendo do tipo de aplicação e do tipo de suporte que se pretende, pode ser feita a escolha. Destacam-se, entre outros, fabricantes como a Philips, Microchip, HID, Motorola, etc. As tecnologias diferem, basicamente, nas frequências utilizadas, que vão desde os 125kHz até os 13.56MHz, no nível de segurança e nos protocolos utilizados [Oliveira, H.; Oliveira, T., 2004].

Chaves eletrônicas

Utilizam um cartão pessoal (*smart cards*) que permite múltiplas aplicações, com características superiores em relação aos cartões de tarja magnética ou códigos de barras, nas mesmas dimensões físicas [Resseler Web, 2005]. Estes cartões apresentam:

- maior segurança, por eliminar a possibilidade da emissão de cartões clones;
- larga vida útil devido a resistências contra ações mecânicas, abrasivas, químicas e interferência eletromagnética;
- maior flexibilidade e capacidade para ler, escrever e armazenar dados;
- não exige um periférico especifico de alto custo e dimensões, apenas para emissão ou alteração de dados no cartão;
- aplicação avançada, isto é, pode ser utilizado como parte de um sistema operacional, como um periférico, memória "flash" de um microcontrolador ou um elemento de autenticação.

Os cartões estão divididos em dois tipos de interface: com contato, seguem a norma ISO 7816 e sem contato que seguem a norma ISO14443A.

Atualmente já existem cartões combinados, que utilizam as duas interfaces de comunicação, com e sem contato, utilizando a mesma área de memória.

Chaveiro de pânico

Através deste dispositivo, o usuário pode discretamente emitir um sinal de emergência para uma central de ocorrências, de modo a acionar lâmpadas, alarmes ou efetuar uma ligação telefônica automática. Ele é também uma forma relativamente simples e rápida de comunicar uma emergência médica a familiares ou a vizinhos, tendo grande utilidade para idosos ou pessoas que necessitam de cuidados especiais.

2.2.3. Sub-sistema de detecção perimetral

O sistema de detecção perimetral é geralmente composto de uma cerca física ou virtual que tem como objetivo detectar e impedir a intrusão de qualquer individuo pela cerca [Bolzani, 2004]. Apresenta-se a seguir alguns dispositivos utilizados neste sistema.

Cerca elétrica

A cerca eletrificada deve detectar a intrusão ou evasão de qualquer indivíduo no menor intervalo de tempo possível com exatidão do ponto de ocorrência. Para evitar falsos alarmes é importante que exista a preocupação com qualquer coisa que possa acionar o alarme [Bolzani, 2004]. A vegetação é um exemplo típico onde se deve ter esse cuidado.

No mercado existem diversos tipos de cercas eletrificadas para segurança residencial que se caracterizam pelos diferentes tipos de fixação. Quanto às centrais eletrificadoras, encontra-se também vários tipos que diferem quanto ao pulso de alta tensão, modo de disparo, memória, programação dos tempos de disparo, etc [Ghn Eletronica, 2005]. Um exemplo de especificação de central eletrificadora é apresentado no Apêndice I.

De acordo com a legislação vigente, cercas eletrificadas só podem ser instaladas em muros com altura mínima de 2,2 metros. A cerca elétrica consiste em um conjunto de 4, 6 ou 8 fios condutores ligados a uma central de choque, que gera um efeito inibidor psicológico. A cerca elétrica é constituída pelos fios sustentados por hastes com isoladores de fácil visualização para inibir invasores. Quando os fios são rompidos ou tocados disparam sirenes, e como opção também podem acionar holofotes e discadores telefônicos. Como fator inibidor, o invasor recebe um pulso de alta tensão (entre 8.000 e 11.000 V dependendo do modelo do aparelho) de baixíssima corrente. O choque é do tipo pulsativo aplicada a cada 1,2 segundos e dura apenas um milésimo de segundo, fazendo com que a descarga elétrica resulte num "tranco" desagradável, mas que não é fatal. Isso torna a cerca elétrica um sistema de proteção perimetral muito eficiente [Produtec, 2005].

Cabo microfônico

As perturbações mecânicas geradas por passos, golpes ou tentativas de arrombamento são transformadas em sinais eletrônicos e analisadas em tempo real por um processador digital que determina a condição de alarme em função dos parâmetros pré-estabelecidos na memória.

Aplicável em estruturas de concreto, muros, lajes ou enterrado em alguns tipos de terrenos (gramados, solos de brita, etc.) como mostra a Figura 2.4.

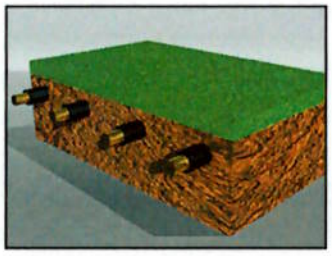


Figura 2.4 – Cabo microfônico

2.2.4. Sub-sistema de sensoriamento externo e interno

Basicamente, os sensores detectam a ocorrência de eventos e enviam esta informação ao controlador que toma a decisão do procedimento a ser adotado [Bolzani, 2004].

Um sensor é, em geral, posicionado a fim de detectar a ocorrência de um evento pontual e enviar a informação na forma de impulsos elétricos para um controlador. Uma falha na detecção, ou mesmo o mau posicionamento do sensor pode ocasionar um erro de identificação do evento causando até uma situação de risco. Os sistemas de controle devem ser projetados sempre pensando na segurança do usuário e, no caso de uma pane ou mau funcionamento, devem tender ao nível de menor energia e maior segurança (por exemplo: ninguém deve ficar preso dentro de uma residência que se incendeia porque o controlador central entrou em pane e travou todas as portas automáticas) [Bolzani, 2004].

Os sensores e detectores em geral trabalham com sinais elétricos analógicos ou digitais, relativos às grandezas monitoradas. Estes sinais são enviados para as placas controladoras ou integrados diretamente no meio físico da rede de comunicação doméstica através de interfaces adequadas. Os detectores de incêndio, por exemplo, são dispositivos que detectam a presença e as variações de parâmetros associados ao fogo – fumaça, calor, chamas – e que transmitem estas informações, em forma de sinais, a uma central que as interpreta. A situação de incêndio que determina a ativação do detector depende de suas características construtivas. Neste caso, a escolha do sensor deve ser conduzida pelo integrador de sistemas de forma a especificar o mais adequado para o ambiente onde vai ser instalado. O tipo de combustão que ali pode ocorrer também deve ser analisado, de modo a combinar os detectores para atingir um melhor ponto de equilíbrio entre a rapidez da ativação com um menor número de falsos alarmes [Bolzani, 2004].

Os sensores são utilizados para monitorar as áreas internas e externas da residência, detectando a presença de pessoas ou intrusos. Atua associado ao controle de acesso e CFTV, enviando um sinal de alarme para a central quando há ocorrência de alguma anormalidade [Bolzani, 2004].

No mercado, os sensores mais utilizados são o magnético de abertura de portas e janelas, de impacto ou vibração, acústico, infravermelho ativo/passivo, de microondas e botões de pânico [Bolzani, 2004].

Apresenta-se a seguir alguns destes dispositivos.

Sensores magnéticos de portas e janelas

Os sensores magnéticos permitem detectar a abertura de portas e janelas. Dentre os tipos existentes, podem ser de sobrepor (Figura 2.5.a), de embutir (Figura 2.5.b) [Alarmes Tucano, 2005]. Estes sensores são compostos de duas partes: uma parte que fica fixa no batente e outra que fica na parte móvel. Caso o sensor perca o contato magnético (no caso de uma porta ou janela ser aberta ou arrombada), o sensor emite um sinal de violação para a central de comando, que dispara o sinal de alarme [Alarm Wolx, 2005].

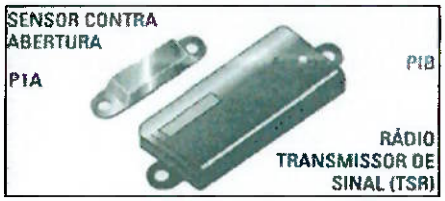


Figura 2.5.a - Sensor de embutir

Figura 2.5.b - Sensor de sobrepor

A Figura 2.6 ilustra uma instalação deste tipo de dispositivo, isto é, o sensor contra abertura (P1A) é colado na porta e o rádio transmissor de sinal (P1B) é colado no batente da porta, em frente ao P1A.

Figura 2.6 – Fixação do sensor magnético de portas

Sensor de impacto

O sensor de impacto ou vibração permite detectar a violação ou pancada brusca na portas ou janelas, acionando o alarme. Estes sensores podem ou não ser temporizados [Practer, 2005].

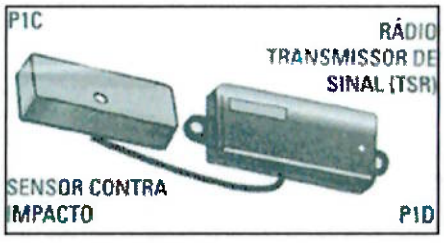


Figura 2.7 – Sensor de impacto

A Figura 2.8 ilustra uma instalação deste tipo de dispositivo, isto é, o sensor contra impacto (P1C) é colado em cima da porta e o rádio transmissor de sinal (P1D) é colado em cima da porta ao lado do P1C.

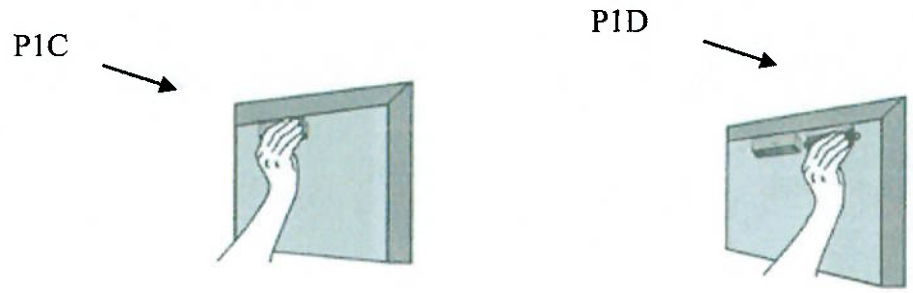
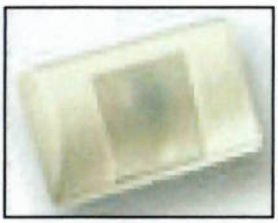


Figura 2.8 – Fixação do sensor de impacto

Sensor infravermelho passivo

O sensor infravermelho passivo permite detectar a movimentação de luz infravermelha na sua área de atuação. A base de seu funcionamento é o detector infravermelho ou PIR, que detecta a variação de luz infravermelha e a transforma numa variação de tensão, interpretada pelo circuito eletrônico. No mercado, existem sensores IVP (infravermelho passivo) de vários tipos, com lente para corredor tipo cortina, para pequenas e grandes distâncias, digital, etc. Existe um tipo para uso em locais com excesso de insetos ou pó que é o tipo "dual", que de maneira simplificada, possui dois sensores lado a lado, que dificultam o disparo indevido. Este tipo de sensor deve ser usado apenas em ambientes internos, de tamanho máximo de 50 metros quadrados. Deve-se evitar o uso em locais muito quentes e onde haja circulação de ar. Em ambientes muito grandes, ou em áreas externas, onde a circulação de ar quente pode "enganar" o sensor, causando alarmes indesejáveis [Alarmes Tucano, 2005].



(a) sensor PIR tipo cortina

(b) sensor PIR digital

(c) sensor PIR *dual*

Figura 2.9 – Alguns tipos de sensores infravermelho passivo

Sensor infravermelho ativo

Já o sensor infravermelho ativo (IVA) possui um circuito que emite luz infravermelha (invisível ao olho humano) e outro que detecta a mesma (RX). O problema do IVA normal é que a variação de distância de uso e também fatores externos tais como chuva, neblina e o próprio sol influenciam sua sensibilidade, ocasionando disparos falsos, principalmente com seu uso em ambientes externos. Para melhorar a eficiência existem modelos que possuem dois emissores de luz infravermelho de freqüências diferentes que são interpretadas pelo RX, além de filtros óticos especiais, o que gera resultados bem melhores, porém o seu custo é bem maior [Alarmes Tucano, 2005].

Estes sensores operam com sinais digitais, convertendo, amplificando e processando o sinal high-low do sensor sem qualquer circuito analógico (Figura 2.10). Também utilizam o processamento *Dual Edge* que separa o sinal de entrada e saída e o nível requerido que cada sinal deve alcançar. Se o sinal de entrada e saída não atingirem o nível requerido, o sinal não é gerado (Figura 2.11) [Paradox, 2004].

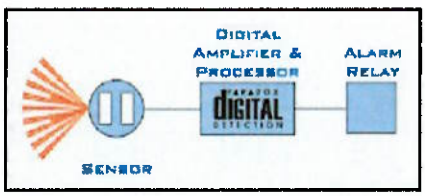


Figura 2.10 – Detecção digital

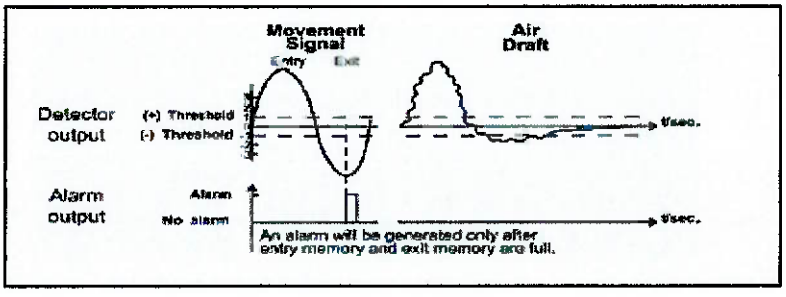


Figura 2.11 – Processamento *Dual Edge*

2.2.5. Sub-sistema de iluminação

Através da automação residencial, a iluminação interna e externa de uma casa pode ser controlada além do interruptor convencional de parede. Sistemas inteligentes podem acentuar os detalhes arquitetônicos de uma sala ou criar ambientes especiais para a leitura de um livro, por exemplo. Ligando ou desligando automaticamente as lâmpadas dos cômodos pode-se afastar os intrusos de uma casa fazendo-a parecer ocupada mesmo na ausência de seus proprietários. Economia de eletricidade é outra vantagem, pois a intensidade de luz é regulada conforme a necessidade e as lâmpadas não precisam operar em sua potência máxima como acontece normalmente [Bolzani, 2004].

Historicamente, os equipamentos de controle de iluminação sempre foram o ponto de partida no processo de automação de uma casa. Os dispositivos que utilizam a tecnologia X.10 já são desenvolvidos há mais de duas décadas e têm obtido certo sucesso em vendas. Atualmente, eles vêm embutidos em sistemas mais complexos de gestão residencial que reúnem também controladores de áudio, vídeo e segurança [Bolzani, 2004].

A iluminação também pode ser gerenciada por um sistema de gestão de energia através de uma programação conjunta com os sensores de luminosidade e de ocupação integrados, alcançando-se uma redução em torno de 30% e 50% no consumo de energia [Bolzani, 2004]. As lâmpadas são acionadas segundo horários previstos e programados conforme a estação do ano, as horas, etc. Em modo automático, acendem quando da entrada de um indivíduo no ambiente onde a iluminação não é suficiente e apagam-se de forma temporizada quando não se detecta a presença de alguém.

Um sistema simples requer alguns módulos X.10 ligados em tomadas simples de parede. Normalmente chamado de sistema *powerline*, o X.10 (denominação comercial) utiliza a própria rede elétrica existente para acionar os pontos de iluminação e ativar tomadas. Estes pontos têm duas formas básicas: uma tomada especial que substitui as convencionais ou um módulo externo que é plugado às tomadas (no caso de abajures, por exemplo). Estes pontos recebem um endereço que é utilizado pelos controladores para identificá-los. Os dispositivos de comando podem ser de vários tipos podendo

variar de interruptores simples até complexos teclados de parede ou consoles de mesa. Cada botão pode enviar sinais de comando do tipo: ligar/desligar ou dimerizar (aumentar/diminuir a intensidade da potência luminosa) os vários pontos de iluminação na residência [Bolzani, 2004].

Outros sistemas mais sofisticados operam através de um cabeamento dedicado podendo interagir com outros sistemas como o de segurança, de ar-condicionado/aquecimento e de entretenimento. Os usuários podem programá-los de tal forma que, com apenas um toque se arme o sistema de segurança e se acendam algumas lâmpadas. Os mais recentes sistemas de controle de iluminação não utilizam fios. Os interruptores se comunicam com as lâmpadas por radio freqüência. São sistemas que podem ser instalados e expandidos com mais facilidade [Bolzani, 2004].

2.2.6. Sub-sistema de redes de comunicação

As redes de comunicação são de grande importância no desenvolvimento, crescimento e sucesso automação residencial, tanto em relação ao conteúdo multimídia quanto ao acesso externo das funções básicas da residência. Várias iniciativas estão sendo tomadas pelas operadoras de telefonia, TV a cabo e satélite no sentido de fornecer serviços de telecomunicações com mais valor agregado. No Brasil, há apenas alguns anos, iniciou-se o processo de modernização da instalação de uma infra-estrutura de comunicações [Bolzani, 2004].

Por outro lado, os diversos problemas sócio-econômicos do país e a falta de recursos de grande parte da população limitam a expansão e modernização das linhas telefônicas que teve sua evolução estagnada assim como aconteceu com a TV a cabo. Devido ainda ao fato de grande parte da população trabalhar fora de sua residência, na economia informal, aumentaram as vendas dos aparelhos celulares que, em 2003, ultrapassou o sistema por fio. Deste modo, para aumentar suas receitas, tanto as companhias telefônicas quanto as provedoras de TV a cabo começaram a agregar serviços à rede de comunicação instalada, aumentando o potencial da casa do usuário ser uma verdadeira célula de processamento de informações com sistemas de áudio, vídeo e dados de altíssima tecnologia [Bolzani, 2004].

Apesar do advento da internet em 1995 e do potencial de diversificação do tipo de comunicação, no Brasil ainda não há diferenciação se a linha de telefone é utilizada para dados ou voz. Assim, até recentemente, o único meio de acesso residencial era através da linha discada que ainda corresponde a maior parte dos gastos com utilização da internet, pois a tarifa é baseada no tempo de conexão, os impulsos [Bolzani, 2004].

Entretanto, existem outras soluções para prover o acesso doméstico à internet de modo mais rápido, confiável e custo reduzido. Algumas formas já estão em uso enquanto outras ainda encontram-se em fase de pesquisa e podem ser organizadas em cinco categorias [Bolzani, 2004]:

- baseadas no sistema de cabos telefônicos;
- baseadas no sistema de TV a cabo;
- baseadas no sistema de distribuição de eletricidade;
- baseadas no sistema sem fio;
- baseadas no sistema de fibras ópticas.

As principais opções para a implantação da rede de comunicações podem ser organizadas segundo a infra-estrutura considerada [Bolzani, 2004]:

- telefônica: ISDN, xDSL;
- TV a cabo;
- energia elétrica: *powerline*;
- sem fio: DBS, celular, MMDS, LMDS;
- fibras ópticas.

2.2.7. Sub-sistema de alarme

Existem diversos tipos sistemas de alarme que se diferenciam pelo nímero de funções e grau de autonomia em sua operação. Em alguns casos o foco está na segurança e confiabilidade enquanto outros são projetados e montados para um ambiente específico [Bolzani, 2004].

Dentre os equipamentos de alarmes, destacam-se:

Central de alarmes

A central de alarme gerencia as múltiplas partições e zonas físicas da residência, os vários códigos de usuários e o registro dos últimos eventos.

Sirene e alarmes sonoros

A função da sirene e alarmes sonoros é emitir sinal de advertência ou aviso quando acionado pelo usuário ou pelo sistema de alarmes.

No mercado existem diversos tipos de sirenes que se caracterizam por diferentes potências sonoras, variedade de tons e aplicações.

Um exemplo de sirene com suas especificações é mostrada na Figura 2.12 [Ghn Eletronica, 2005].

Especificações:

- 1 tom;
- DC: de 9 a 12 volts;
- Consumo da Corrente: 200 mA (+/- 10%);
- Dimensões: Ø55 x 63 mm;
- 112 dB a 1 metro (12V DC);
- 120 dB a 30 cm(12V DC);

Figura 2.12 – Sirene MA-11 Fire

Discadoras automáticas

Possibilitam o envio de mensagens de alarme ou informações sobre um acontecimento para um usuário remoto ou uma central remota de atendimento das ocorrências.

2.3. Integração do sistema de segurança em residências inteligentes

Um dos pontos principais no desenvolvimento de sistemas de automação para residências inteligentes é a integração dos sistemas e serviços. As informações de sensores utilizados pelo equipamento de segurança podem ser utilizadas também para

controlar a iluminação dos ambiente. De igual forma, as informações dos sensores de condicionamento do ar podem indicar a ocorrência de incêndio. Assim, os sistemas de segurança podem fazer mais do que pedir ajuda. Com uma rede de comunicações de dados utilizada para este fim, os mesmos sensores que detectam movimento, fogo, ou iluminação podem ativar um número variado de ações. Caso haja a necessidade, o sistema de segurança pode interferir no controle do ar condicionado e ventilação, abrindo as portas e janelas. Ele também pode enviar sinais para ligar e desligar a iluminação de acordo com os estado dos detectores de movimento e atuar em conjunto com o funcionamento das câmeras de vigilância. Deve-se assim estudar um modelo adequando a verificação e validação destas propostas, implicar em custos adicionais com equipamentos, minimizando alterações na rede física de comunicações [Bolzani, 2004].

O programa de controle que gerencia os sistemas domóticos de uma residência, na maioria das vezes, é implementado pelos próprios provedores de serviços. Por exemplo: a empresa responsável pela instalação do sistema HVAC pode fornecê-lo junto com o equipamento e instalá-lo no computador central ou em algum outro equipamento de supervisão geral dos serviços da residência. A hipótese é que os vários *softwares* atuariam em harmonia dentro da mesma rede de comunicação residencial. Entretanto, na prática isso não existe, isto é, antes é necessário definir uma padronização e as formas de inter-operabilidade tanto para o *hardware* como para o software [Bolzani, 2004].

CAPÍTULO 3

SISTEMAS A EVENTOS DISCRETOS E REDE DE PETRI

Este capítulo trata dos conceitos fundamentais envolvidos no presente trabalho. Vale ressaltar que a base teórica de sistemas a eventos discretos, redes de Petri e suas extensões, baseia-se nos trabalhos de Gustin [1999] e Miyagi [1996].

3.1. Sistema a eventos discretos

Definição: sistema a eventos discretos (SED) é um sistema dinâmico que evolui de acordo com a ocorrência de eventos, em intervalos de tempo em geral irregulares e desconhecidos que resultam na mudança abrupta do estado do sistema [Cury, 2001].

Em oposição aos sistemas de variáveis contínuas os SEDs são caracterizados por apresentarem variáveis de estado discretas, serem dirigidos a eventos e não serem descritíveis por equações diferenciais (ou a diferenças) [Ho, 1989]. A rigor, a primeira condição relacionada acima não caracteriza propriamente um sistema discreto, visto que sua inobservância não impede que um sistema apresente dinâmica discreta. Contudo na maioria dos casos estudados na Engenharia esta característica está presente. O segundo ponto é talvez o mais importante da caracterização dos sistemas a eventos discretos. Sua dinâmica é dirigida a eventos, ou seja, o que determina a evolução do sistema é a ocorrência de eventos e não simplesmente o passar do tempo. É óbvio que, embora o tempo continue sendo um parâmetro importante na caracterização da dinâmica do sistema, ele agora não é determinante.

Os principais modelos utilizados para descrever os SEDs:

- rede de Petri com e sem temporização;
- rede de Petri controlada com e sem temporização;
- cadeia de Markov;
- teoria das filas;
- processo semi-Markovianos generalizado (GSMP) e simulação;
- álgebra de processos;

- álgebra Max-Plus;
- lógica temporal e lógica temporal de tempo real;
- teoria de linguagens e autômatos (Ramadge-Wonham).

3.2. Conceito e aplicações de rede de Petri

A seguir apresenta-se os conceitos principais de rede de Petri necessários para a modelagem de sistema de segurança. É apresentado o PFS/MFG (Production Flow Schema/Mark Flow Graph) que é uma interpretação da rede de Petri efetiva para a modelagem, análise e especificação de SEDs.

3.2.1. Rede de Petri

A rede de Petri deve o seu nome ao trabalho de Carl Adam Petri que no seu doutorado, apresentou um tipo de grafo bipartido com estados associados para estudar a comunicação entre autômatos [Murata, 1989]. O seu desenvolvimento posterior foi catalisado pelas suas numerosas potencialidades de modelagem, em especial: sincronização de processos, concorrência, conflitos e partilhamento de recursos. Desde então, têm sido desenvolvidos trabalhos teóricos e aplicações envolvendo a rede de Petri tendo estes estudos levado, quer a um desenvolvimento das técnicas de análise da rede de Petri e sua aplicação prática, quer ao desenvolvimento de variantes do modelo seminal da rede de Petri tendo em vista aplicações específicas.

Como ferramenta matemática e gráfica, a rede de Petri oferece um ambiente uniforme para a modelagem, análise formal e simulação de SEDs, permitindo uma visualização simultânea da sua estrutura e do seu comportamento. Mais especificamente, a rede de Petri modela dois aspectos dos SEDs, eventos e condições, bem como, as relações entre eles. Segundo esta caracterização, em cada estado do sistema verificam-se determinadas condições. Estas podem possibilitar a ocorrência de eventos que por sua vez ocasionam a mudança de estado do sistema [Peterson, 1981].

3.2.2. Características e vantagens

Em [Hasegawa, 1996] destacam-se as seguintes características e vantagens desta técnica:

- representa a dinâmica e a estrutura do sistema segundo o nível de detalhamento desejado;
- identifica estados e ações de modo claro e explícito, facilitando com isto a monitoração do sistema em tempo real;t
- têm a capacidade para representar de forma natural as características dos SED (sincronização, assincronismo, concorrência, causalidade, conflito, compartilhamento de recursos, etc.);
- associa elementos de diferentes significados numa mesma representação, ou segundo o propósito do modelo (avaliação de desempenho, implementação do controle, etc);
- oferece um formalismo gráfico que permite a documentação e monitoração do sistema, facilitando assim o diálogo entre o projetista e as pessoas que participam no processo de projeto ou de análise do comportamento do sistema (projetista, operador, gerente, etc.);
- se constitui como uma teoria, bem fundamentada para a verificação de propriedades qualitativas;
- possui uma semântica formal e precisa que permita que o mesmo modelo possa ser utilizado tanto para a análise de propriedades comportamentais (análise quantitativa e/ou qualitativa) e avaliação do desempenho, assim como para a construção de simuladores discretos e controladores (para implementar ou gerar códigos para controle de sistemas). Além de servir para verificar comportamentos indesejáveis como bloqueio, limitação, etc;
- incorpora conceitos de modelagem do tipo refinamento (*top down)* e do tipo composição modular (*bottom up)* através de técnicas como: modularização, reutilização, refinamento, etc.

Como uma ferramenta matemática, um modelo em rede de Petri pode ser descrito por um sistema de equações lineares, ou outras relações matemáticas que refletem o

comportamento do sistema [Zurawski & Zhou, 1994], o qual possibilita a análise formal do mesmo. Esta característica permite realizar a verificação formal das propriedades comportamentais do sistema.

Assim, a rede de Petri se constitui como uma poderosa ferramenta para o modelagem e análise de SEDs. Entretanto, na modelagem de sistemas complexos e com diferentes níveis de abstração se evidencia um ponto fraco em uma de suas principais características: sua visualização gráfica. Desta maneira, verifica-se que é adequado que a modelagem inicial seja realizada utilizando interpretações não formais e, a partir deste modelo seja conduzido um detalhamento gradativo e com interpretações formais. E, é neste contexto que as técnicas do PFS (Production Flow Schema) e do MFG (Mark Flow Graph) [Hasegawa et al., 1988] são consideradas. O PFS e o MFG são extensões interpretadas da rede de Petri (de modo que herdam o poder de representação e as técnicas formais de análise de grafos), próprias para aplicação em diferentes níveis de modelagem, análise e controle de SEDs.

Estas considerações conduziram à escolha desta metodologia como ferramenta para a modelagem do sistema em estudo.

Modelagem com redes de Petri

Quando se modela um sistema através de uma rede de Petri, está necessariamente criando-se uma interpretação na forma de rede. É essa interpretação que efetua a ligação do modelo abstrato que qualquer rede de Petri representa, com o sistema concreto que se pretende modelar [Reisig, 92].

3.2.3. PFS/MFG

O PFS/MFG consiste num procedimento para a modelagem de sistemas, seguindo uma abordagem sistemática, racional e hierárquica, com base em sucessivos refinamentos para conceber e detalhar o modelo de forma progressiva e estruturada. Inicialmente o modelo conceitual do sistema (representando um alto nível de abstração do sistema sem detalhamento de sua dinâmica) é desenvolvido com o PFS. Nesta etapa o propósito é modelar as principais características das funções que serão consideradas no sistema. A

ênfase está na identificação dos componentes ativos e passivos do sistema, assim como do fluxo de itens (material e/ou informação) entre estes elementos.

Para a descrição funcional do sistema, os elementos do grafo PFS são então detalhados. Este detalhamento pode gerar sub-grafos totalmente em PFS ou sub-grafos em MFG ou sub-grafos híbridos (PFS/MFG) com alguns elementos em PFS e outros em MFG.

Na modelagem do comportamento dinâmico do sistema, o modelo em PFS é convertido progressivamente em um modelo em MFG (ou uma rede de Petri interpretada adequada) que detalha o funcionamento das diversas partes do sistema (até o nível desejado), através da evolução dinâmica da marcação do grafo [Miyagi, 1996].

Quando são utilizados equipamentos de controle programáveis, o detalhamento das atividades pode ser realizado até um nível de operação isto é, onde as ações são especificadas pelo programa de controle disponível ou a ser implementado.

O PFS/MFG como técnica para modelar SEDs, originalmente foi proposta para a aplicação em sistemas de manufatura, e neste campo tem sido usada para tratar sua modelagem e análise com sucesso [Miyagi, 1988; Santos Filho, 1993; Arakaki, 1993, Liu, 1993; Kagohara, 1998]. Entretanto esta técnica pelas suas características pode ser estendida ao caso de sistemas segurança residencial, onde através de uma visão macro e conceitual do sistema, os diferentes sistemas e suas funções são detalhadas até o nível de interface com os dispositivos físicos instalados na residência [Arakaki et al., 1998].

PFS

O PFS (Production Flow Schema) [Hasegawa et al., 1988; Miyagi, 1988; Silva & Miyagi, 1995], é uma classe de rede canal-agência [Reisig 1992] devidamente interpretada e constitui uma técnica para representar o nível conceitual mais alto de abstração do sistema sem detalhamento do comportamento dinâmico.

O PFS caracteriza um sistema a partir de seus elementos ativos e fluxo de materiais e informações dentro de um processo. Esta abordagem baseia-se no princípio de que um sistema é composto por elementos ativos que realizam transformações e elementos

passivos que realizam a distribuição de itens (materiais ou informações), existindo portanto uma inter-relação entre estes elementos para a realização efetiva dos fluxos presentes no sistema. Deve-se salientar que o PFS, distintamente da rede de Petri não possui o conceito de marcação, pois é um modelo conceitual do sistema sem descrição de sua dinâmica.

Os elementos estruturais do PFS são os seguintes:

- atividade: representa um componente ativo do sistema capaz de realizar transformações, isto é, ações. As *atividades* podem agregar uma ou mais operações (não explícitas no presente nível de abstração). Graficamente, corresponde a um macroelemento delimitado por colchetes e com inscrições em linguagem natural ou formal para especificá-lo. Cada *atividade* pode ser refinada em *sub-atividades* com as suas respectivas interações. Uma *atividade* pode ser iniciada ou finalizada pela ocorrência de um ou mais eventos exclusivos [Sugisawa, 1998]. Sua representação é apresentada na Figura 3.1.

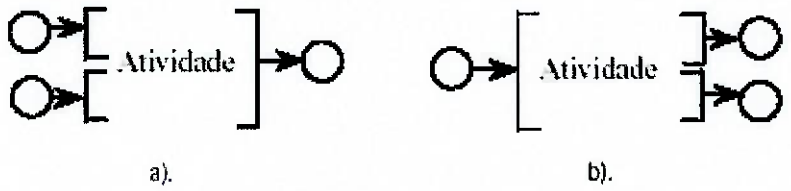


Figura 3.1 a) Início da *atividade* devido a ocorrência de dois eventos;

b) Término da *atividade* devido a ocorrência de dois eventos.

- inter-atividade ou distribuidor: representa um componente passivo, capaz de armazenar, permanecer em determinados estados ou tornar os itens visíveis. É indicado graficamente por uma circunferência. Uma *inter-atividade* deve existir sempre entre duas *atividades* que estejam relacionadas;
- arco: conectam *atividades* a *inter-atividades* e vice-versa representando o fluxo de materiais e/ou informações. Os *arcos* indicam uma relação lógica, entre os componentes. Se a conexão se faz pela parte externa da *atividade,* indica um

fluxo principal de itens no sistema e se é realizada pela parte interna, indica um fluxo secundário (este fluxo não é obrigatório). Graficamente corresponde a uma seta.

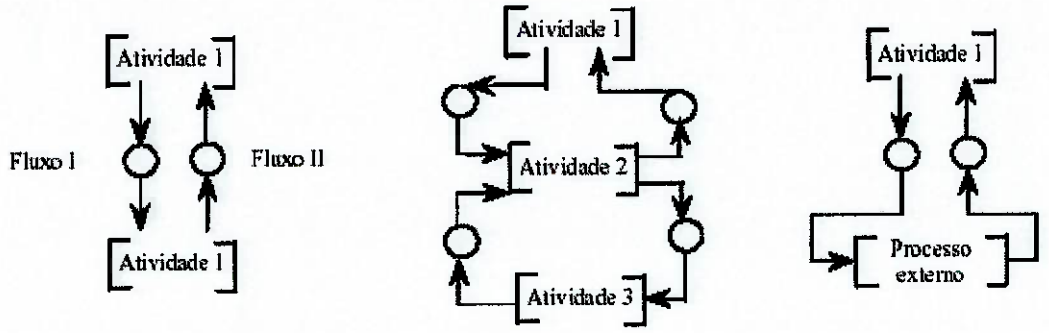
Deve-se observar que elementos de um mesmo tipo não podem ser conectados diretamente uns aos outros. Além disso, cada um dos componentes recebe inscrições em linguagem natural, indicando sua interpretação específica para o modelo elaborado.

Neste nível de descrição, algumas características de SEDs, que ficam explicitadas nos modelos em PFS são:

- sequência: indica a relações de precedência entre as *atividades*, onde o início de uma só pode ocorrer ao término da anterior;
- sincronização: caso no qual mais de um elemento *inter-atividade* se encontram à entrada de uma *atividade*. Refere-se à condição de que esta *atividade* só tem início (fim) se os elementos *inter-atividade* estiveram em condições próprias para iniciar (concluir) a *atividade*;
- paralelismo: quando mais de um elemento *inter-atividade* se encontraram à saída de uma *atividade*, assim ocorre paralelismo entre as *atividades* na seqüência desses elementos *inter-atividade*;
- concorrência: situação em que existem duas ou mais *atividades* com fluxos derivados (decisão) ou convergentes a um único elemento *inter-atividade*. Representa o fato que os elementos de um fluxo podem ter mais de uma opção quanto à próxima *atividade*; sendo preciso, neste caso, que um processo de decisão deva ser associado à seleção de uma das possibilidades;
- compartilhamento de recursos: é um caso particular de decisão, onde várias *atividades* podem vir a solicitar, simultaneamente, o mesmo recurso.

O PFS representa as funcionalidades específicas de um sistema, enfocando uma forma de organização das *atividades* (ou seja, características de seqüência, sincronização, decisão, etc.) e recursos alocados para executar estas. Assim, os diversos modos como as *atividades* são coordenadas e os recursos são atribuídos às *atividades* determinam as diferentes funcionalidades.

Além das estruturas apresentadas (paralelismo, concorrência, etc.), definidas pelo fluxo principal, os fluxos secundários podem também definir relações como [Liu, 1993]: comunicação assíncrona para troca de informações entre *atividades* (Figura 3.2.a), comunicação síncrona, onde as *atividades* são sincronizadas através de outra *atividade* (Figura 3.2.b) e, chamadas de procedimentos externos, na qual é se tem a utilização de um mesmo processo (exemplo um gerenciador de banco de dados) por várias *atividades* (Figura 3.2.c).



a) Comunicação Assíncrona de *atividades*

b) Comunicação Síncrona entre *atividades*

c) Chamada entre procedimento externo

Figura 3.2 – Interpretação típica dos fluxos secundários

A abordagem hierárquica, permitida pelo PFS, faz com que o modelo possa ser detalhado passo a passo através de refinamentos sucessivos das *atividades*. Para realizar este refinamento podem ser usadas as estruturas descritas anteriormente e as suas combinações. Assim, por exemplo, sempre que o fluxo seja dispersado em dois ou mais, em situações de paralelismo ou de concorrência, este deverá convergir respectivamente, em forma de sincronização ou em convergência para um elemento *inter-atividade*, conforme é apresentado nas Figuras 3.3.a e 3.3.b. Outro refinamento possível é o que carateriza um "loop" (ciclo repetitivo), onde um elemento *inter-atividade* possui duas possibilidades: realizar a *atividade* interna 1 ou encerrar a *atividade* global, esta estrutura é indicada na Figura 3.3.c.

a) *Inter-atividade* em sincronização

b) *Inter-atividade* em convergência

c) "loop"

Figura 3.3 – Exemplo de *inter-atividades*

A Figura 3.4 mostra um exemplo de aplicação do detalhamento do PFS referente a função de reconhecimento e identificação que aplica a relação de concorrência entre atividades.

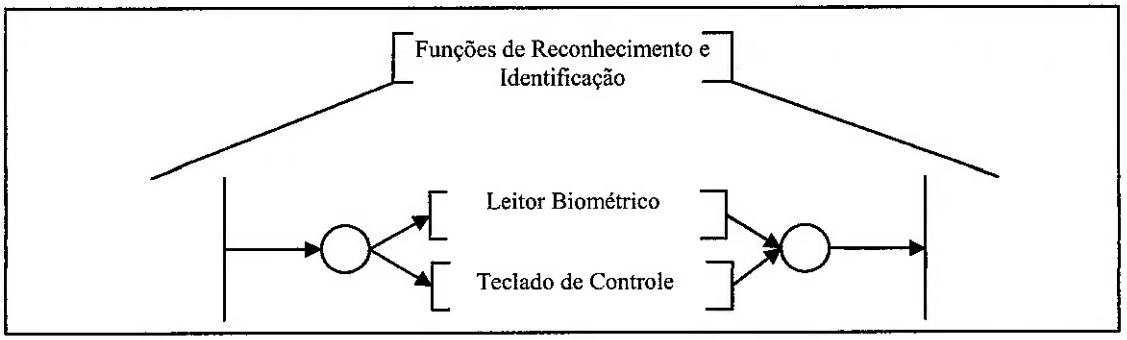


Figura 3.4 – Exemplo de aplicação das relações de concorrência entre atividades

A Figura 3.5 mostra um exemplo de aplicação do detalhamento do PFS referente a "ação externa" que aplica a relação de paralelismo entre as atividades.

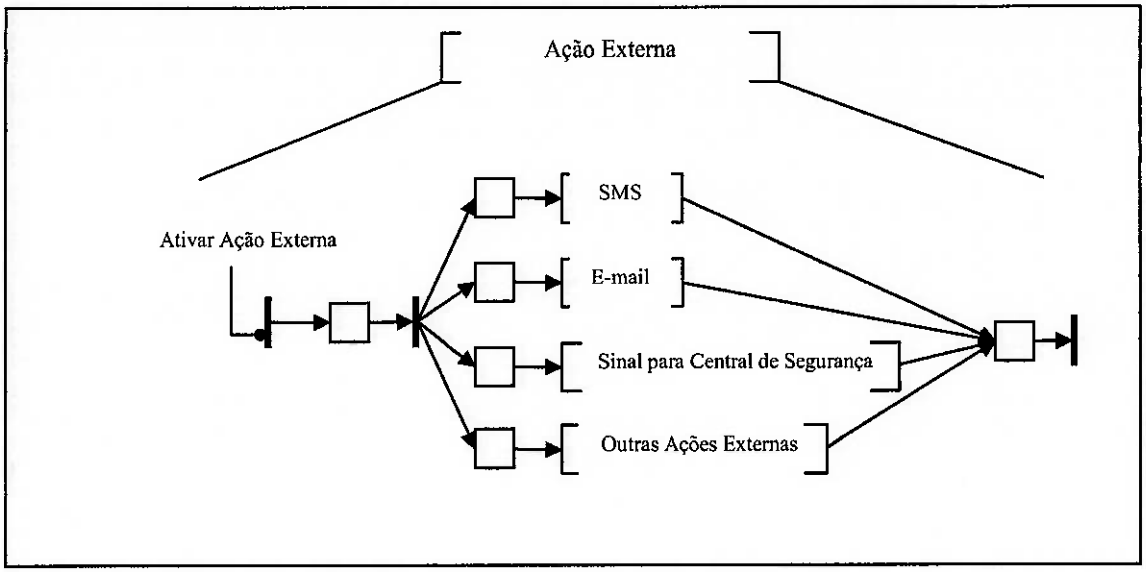


Figura 3.5 – Exemplo de aplicação das relações de paralelismo entre atividades

3.3. Observações finais do capítulo

Neste capítulo apresentou-se a rede de Petri como uma das técnicas que existem para a modelagem e análise de SEDs, dentro do qual foi caracterizado o sistema de segurança residencial, e que se destaca por seu potencial como uma técnica uniforme de modelagem, sua facilidade de interpretação, modularização, e representação hierarquizada. Dentro deste contexto foi selecionado o PFS/MFG (Production Flow Schema/Mark Flow Graph) que permite através de um abordagem *top-down* sistematizar e racionalizar a construção de grafos até a obtenção do modelo funcional do sistema em MFG que é uma interpretação da rede de Petri, efetiva para modelar e especificar o comportamento dinâmico de SEDs, explicitando sua comunicação com elementos externos.

CAPÍTULO 4

METODOLOGIA PARA MODELAGEM DE SISTEMAS DE SEGURANÇA

Neste capítulo é apresentada a metodologia adotada para a modelagem de sistemas de segurança em residências inteligentes, indicando as etapas que devem ser consideradas. A metodologia utilizada é uma adaptação da metodologia proposta por Miyagi [1996].

4.1. Metodologia aplicada

De acordo com Gustin [1999], a metodologia deve auxiliar e orientar adequadamente o projeto de sistema de segurança para automação residencial na medida em que deve fornecer o suporte necessário para o desenvolvimento do modelo deste sistema, considerando uma eficiente integração com outros sistemas da residência inteligente (seja residência a ser construída, onde se define os parâmetros iniciais necessários para a instalação do sistema de segurança ou, para tornar inteligente uma residência convencional). Portanto, esta metodologia deve organizar e estruturar as etapas de trabalho em forma sistemática com a finalidade de auxiliar no projeto deste sistema, outorgando suporte adequado à flexibilidade do sistema que esta classe de residências deve apresentar.

Considerando que o sistema de segurança para residências inteligentes tem como finalidade básica fornecer ao usuário praticidade, conforto e segurança, através de sua integração eficiente com outros sistemas residenciais, é importante que sua modelagem represente o sistema de forma adequada com relação a aspectos que possam afetar seu serviço (dinâmica de funcionamento, estratégias de controle que permitem a sua integração com outros sistemas da residência, etc.) com a finalidade de permitir uma posterior análise do mesmo.

A metodologia para a modelagem de sistemas de segurança pode ser dividida nas etapas gerais ilustradas na Figura 4.1.

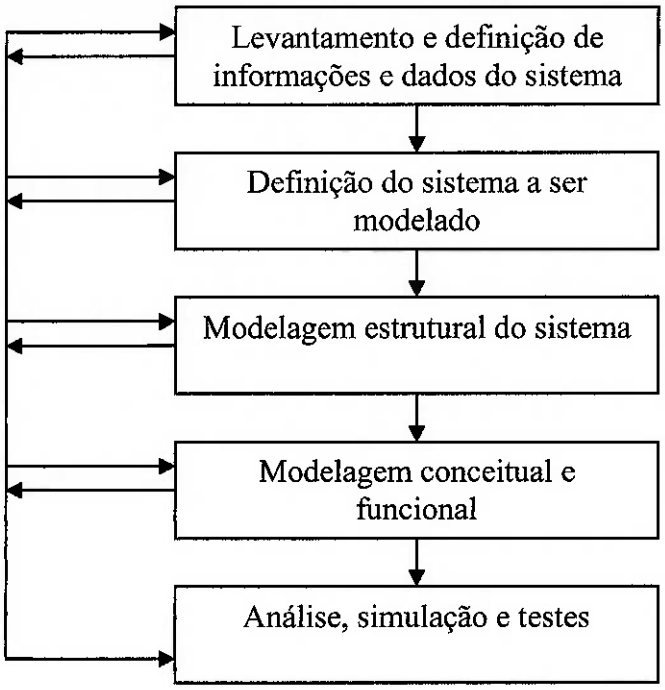


Figura 4.1 - Metodologia para a modelagem.

Etapa 1 - Levantamento e definição de informações e dados do sistema de segurança

Nesta etapa procura-se conhecer o sistema de segurança através do levantamento das informações deste, as quais servem também como um meio para realizar uma análise preliminar e identificar os dados relevantes ao sistema, pertinentes para a modelagem do mesmo e que permitam caracterizar os elementos no nível qualitativo e quantitativo, tanto para o caso de uma residência já construída ou em fase de projeto.

Passo 1.1 - Análise das funções e objetivos

Primeiramente, deve-se fazer uma análise do sistema de segurança que se pretende implantar, definindo quais objetivos e funções que o sistema deve atender.

É recomendável que se inicie a análise pelos objetivos básicos, detalhando as funções que o sistema deve possuir visando alcançar os objetivos. As funções definidas também

devem considerar aspectos como: prevenção ou dissuasão, detecção e alarmes, reconhecimento ou identificação, retardo, reação e integração dos sistemas.

Passo 1.2 - Definição dos sistemas

Após a definição das funções e objetivos, que o sistema de segurança proposto deve apresentar, deve-se definir os sub-sistemas que são necessários e farão parte do sistema de segurança, por exemplo: sistema de vigilância com CFTV, sistema de sontrole e automação de acesso, sistema de detecção perimetral, sistema de sensoriamento externo e interno, sistema de redes de comunicação, sistema de iluminação e sistema de alarme.

Cada sub-sistema deve executar totalmente ou parcialmente todas as funções e objetivos pré-definidos.

Passo 1.3 - Definição das estratégias de controle

Uma vez que definidos os sub-sistemas que irão compor o sistema de segurança, de acordo com [Bolzani, 2004], para um projeto de sistema de segurança, deve-se definir as estratégias de controle do sistema.

Passo 1.4 - Levantamento dos dispositivos do sistema de segurança

Deve-se fazer um levantamento dos vários dispositivos, existentes ou que devem ser projetados, que atendam as necessidades do sistema de segurança.

Ao final devem-se gerar os seguintes documentos:

- diagrama estrutural: mostrando os principais componentes físicos e lógicos do sistema de segurança;
- lista preliminar de dispositivos: detalhando as características de cada componente.

Etapa 2 – Definição do sistema de segurança a ser modelado

Nesta etapa, as informações levantadas são analisadas e são avaliadas a validade e viabilidade técnica do sistema, considerando as normas e legislação relacionadas com os sistemas de segurança e o tipo e função da residência onde serão instalados, além da tecnologia disponível, para se obter uma definição mais precisa do que é requerido para este.

Dentre análises, destaca-se:

- definição das funções de segurança de acordo com as situações operacionais consideradas. Por exemplo: nível primário de segurança e nível secundário de segurança de acordo com a presença ou não dos moradores;
- definição de zonas, isto é, ambientes objeto do sistema de segurança;
- definição dos sub-sistemas de segurança e respectivas funções.

Ao final, deve-se gerar um documento contendo:

- Lista com a especificação técnica de cada dispositivo que será utilizado.

Etapa 3 – Modelagem estrutural do sistema de segurança

Esta etapa consiste no desenvolvimento do modelo estrutural do sistema de segurança, onde são identificadas e explicitadas todas as partes que o compõem, considerando-os dentro do contexto das residências inteligentes e levando em conta a arquitetura adotada para o sistema de controle.

Nesta etapa, o sistema de segurança é abordado de forma bipartida, dado que este pode ser representado mediante a inter-conexão de dois sub-sistemas fundamentais que se comunicam cooperativamente. Estes sub-sistemas representam a parte operativa relacionada ao objeto de controle e a parte de controle relacionada ao sistema de controle [Silva, 1985] (vide Figura 4.2).

Esta decomposição do sistema consiste em estabelecer uma distinção entre o sub-sistema de execução (parte operativa) e o sub-sistema de coordenação (parte de controle). Assim, a parte operativa envia para a parte de controle informações sobre seu

estado (que possibilitam a realização do controle) e, a parte de controle de acordo com estas informações retorna à primeira ordens de operação através dos atuadores. Desta forma, impõe-se o comportamento dinâmico desejado de acordo com a especificação das ordens de comando externas.

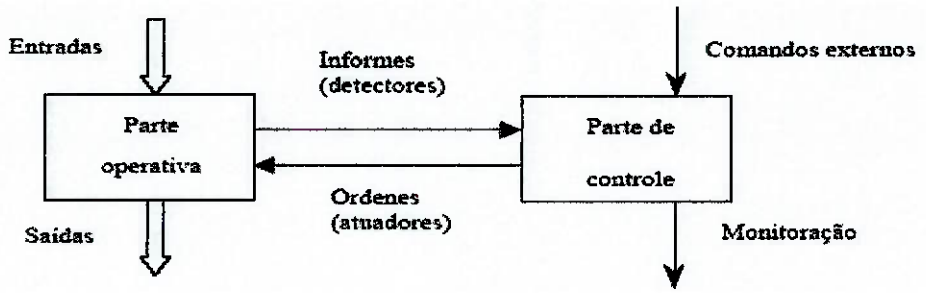


Figura 4.2 - Decomposição da descrição de um sistema de segurança em parte operativa e parte de controle

Esta decomposição permite tratar a complexidade do sistema de segurança e simplifica a construção do modelo global do sistema.

Nesta etapa, os componentes da parte de controle são considerados de acordo com o diagrama apresentado na Figura 4.2, levando em conta os dispositivos de controle para cada ambiente da residência.

No modelo estrutural resultante é indicada a interação entre as diferentes partes do sistema, onde cada um dos elementos estruturais deste pode ainda ser dividido em módulos, para facilitar a modelagem do sistema.

Etapa 4 – Modelagem conceitual e funcional do sistema de segurança

Nesta etapa, a modelagem de cada um dos elementos estruturais do sistema é realizada de forma sistemática e hierárquica, sendo que inicialmente aborda-se o sistema no nível conceitual para em seguida fazer um refinamento do mesmo e obter seu modelo funcional. Assim, inicialmente trata-se o sistema num nível de abstração que não considera o seu comportamento dinâmico e, posteriormente, realiza-se o detalhamento de modo progressivo e até derivar o modelo funcional do sistema.

O modelo conceitual do sistema é particularmente importante para tratar os problemas de interpretação das informações obtidas (as quais muitas vezes são subjetivas), ao auxiliar a organização das idéias e o conhecimento do sistema e permitindo a descrição e compreensão deste ao descrever as principais inter-relações e funções de seus diferentes componentes, para depois derivar uma especificação funcional adequada.

Para esta etapa é adotada como técnica de modelagem o PFS utilizado dentro do contexto do PFS/MFG.

A elaboração de um modelo em PFS adequado e correto nesta etapa da metodologia é de fundamental importância não somente porque ajuda a organizar as idéias e informações coletadas, mas também porque os modelos subseqüentes são baseados no refinamento destes modelos. Assim, os modelos construídos são avaliados e revisados em função da satisfação plena das características do sistema definido. Nessas avaliações podem ser detectadas falhas na construção dos modelos, ou até mesmo falhas no levantamento das informações, o que pode implicar em novos levantamentos e até na redefinição do sistema.

Neste nível, deve-se inicialmente identificar as principais atividades realizadas em cada um dos elementos considerados no modelo estrutural do sistema, sendo importante ter em conta as inter-relações entre estes elementos, definindo as suas respectivas funções dentro do sistema. A representação é realizada por elementos que se inter-relacionam através dos fluxos definidos pelo sistema.

Nos sistemas de segurança estas inter-relações podem ser identificadas como fluxos de informações na entrada e saída de cada sub-sistema.

Por sua vez, a modelagem funcional compreende a descrição do comportamento dinâmico do sistema. Para a consecução deste modelo é adotado o MFG [Miyagi, 1996].

A utilização desta técnica de modelagem permite a representação explícita dos estados alcançáveis do sistema e da troca de sinais entre o controlador e o objeto de controle. Sua aplicação baseia-se na representação do fluxo de informações. Assim, o controlador

recebe informações e envia os sinais pertinentes aos dispositivos de controle a partir de *arcos de sinal de saída* no sentido de habilitar a realização de uma determinada tarefa e, em contra partida, recebe informações de confirmação do término da tarefa a partir de *portas externas* associadas aos dispositivos de controle, deixando livre o controlador para a realização da etapa seguinte de controle.

Desta forma, realiza-se a integração das diversas partes estruturais do sistema através do controle do fluxo de informação.

A especificação funcional do sistema na forma do grafo PFS/MFG obtida nesta etapa serve para definir os requisitos para o projeto do sistema. Uma análise destes requisitos permite até mesmo alterar os parâmetros inicialmente adotados para o sistema.

Etapa 5 – Análise e simulação do funcionamento do sistema de segurança

Os modelos são assim avaliados com a finalidade de verificar se eles representam adequadamente as especificações do sistema concebido, de tal forma que seu comportamento dinâmico seja coincidente com o comportamento esperado. Esta análise pode implicar em correções do modelo.

Nesta etapa é realizada a análise dos modelos gerados através de simulações funcionais e comportamentais do sistema. Esta etapa pode ser conduzida com o apoio de ferramentas como o HPSim (software para simulação de rede de Petri) que auxiliam na edição da rede de Petri, análise estrutural e comportamental da rede.

A simulação caracteriza os diferentes cenários e a dinâmica de funcionamento de uma residência inteligente. Através da simulação pode-se analisar diferentes alternativas comportamentais do sistema visando melhoria, acréscimo de eficiência e visibilidade das reações do sistema.

CAPÍTULO 5

EXEMPLO DE APLICAÇÃO

5.1. Aplicação da metodologia de modelagem

Este capítulo apresenta um exemplo de modelagem de sistema de segurança para residências inteligentes através da aplicação da metodologia descrita no capítulo 4.

Como na automação residencial, as soluções são pessoais e dirigidas, variando de usuário para usuário, o modelo gerado neste trabalho procura ser relativamente genérico, para que possa ser utilizado como base em outros projetos. Como acontece em muitas situações, o fator econômico pode limitar as especificações das soluções.

Etapa 1 - Levantamento e definição de informações e dados do sistema de segurança

Passo 1.1 - Análise das funções e objetivos

Deve-se assegurar, que as funções desempenhadas pelo sistema de automação residencial, alcancem os objetivos previstos, através da introdução de vários níveis de automação em áreas distintas e com equipamentos diversos [Kroner, 1997].

Os principais objetivos, descritos no capítulo 2, de satisfação, racionalização de custos, efetividade na recepção e transmissão de informações e confiabilidade devem ser evidentemente satisfeitos pelo sistema.

Dentro de sistemas de segurança é imprescindível criar soluções que sejam não somente compatíveis, mas também complementares com outros sistemas residenciais. O sistema de segurança deve cumprir fundamentalmente os seguintes pontos considerados básicos [Bolzani, 2004]: prevenção ou dissuasão, detecção e alarmes, reconhecimento ou identificação, retardo, reação e integração dos sistemas.

O sistema deve ser capaz de identificar várias situações e reagir a elas. Finalmente, ele deve atuar em conjunto com os outros sistemas que controlam os demais serviços residenciais [Bolzani, 2004].

Tabela 5.1 – Funções do sistema de segurança

Prevenção ou Dissuasão	Com o propósito de impedir a intrusão ou ataque, o sistema deve ser capaz de gerar barreiras físicas ou virtuais, impedindo acessos e executando ações.
Detecção e Alarmes	O sistema deve ser capaz de coletar sinais que indiquem perturbações e alterações no ambiente ou em dispositivos.
Reconhecimento e Identificação	O sistema deve ser capaz de reconhecer o usuário do não usuário.
Retardo	O sistema deve ser capaz de analisar e processar as informações, no intuito de minimizar falsos alarmes e detectar falhas no próprio sistema.
Reação	O sistema deve ser capaz de efetivamente executar ações que detenham a intrusão ou ataque.
Integração de Sistemas	O sistema de segurança deve ser integrado com seus respectivos subsistemas e com outros sistemas que a residência inteligente possa ter.

A residência tem que possuir características que atendam às expectativas dos usuários. Assim, o projeto residencial tem que satisfazer a diferentes necessidades através de uma abordagem que se adapta a infra-estrutura dimensionada e que facilite a instalação dos sistemas. Assim, o modelo gerado poderá ser aproveitado também para situações futuras que envolvem novos conceitos de segurança automatizada [Bolzani, 2004].

Passo 1.2 - Definição dos sistemas

Para atender aos objetivos e as funções básicas, o sistema é caracterizado pelos seguintes sub-sistemas de um sistema de segurança para residências inteligentes:

- sub-sistema de vigilância com CFTV: funções de reconhecimento e detecção;
- sub-sistema de controle e automação de acesso: funções de identificação;
- sub-sistema de detecção perimetral: funções de prevenção e reação;
- sub-sistema de sensoriamento interno e externo: funções de detecção;
- sub-sistemas de iluminação: funções de prevenção, dissuasão e reação;
- sub-sistema de redes de comunicação: funções de reação e retardo;
- sub-sistema de alarme: funções de alarme.

Passo 1.3 - Definição das estratégias de controle

As estratégias, definidas juntamente com a [Aureside, 2005], são baseadas em sistemas de segurança existentes e que são amplamente aplicadas no mercado brasileiro.

Nesta aplicação, uma das estratégias de controle é a divisão em dois grupos de ações: nível primário e secundário. As ações no nível primário definem e afetam as ações do nível secundário que serão executadas.

- estratégia de zonas: para otimizar a relação entre usuários e equipamentos, os espaços físicos serão divididos em sub-espaços virtuais, proporcionando tratamento diferenciado em relação ao controle dos sistemas e padrões de sensoriamento;
- estratégia de integração dos sistemas: centralizar o gerenciamento da segurança em um único sistema de controle, capaz de possibilitar a interoperabilidade entre os sub-sistemas. Os sistemas devem ser integrados devendo ocorrer troca de informação entre eles, isto é, as ações ou sinais de um sistema podem afetar as ações de outro sistema. Além disso, deve haver a integração do controle de todos os sistemas, possibilitando o acionamento, controle e monitoração dos cada dispositivo através de um controle ou de um acesso remoto.

Passo 1.4 - Levantamento dos dispositivos do sistema de segurança

A Figura 5.1 apresenta o diagrama estrutural do sistema de segurança considerado.

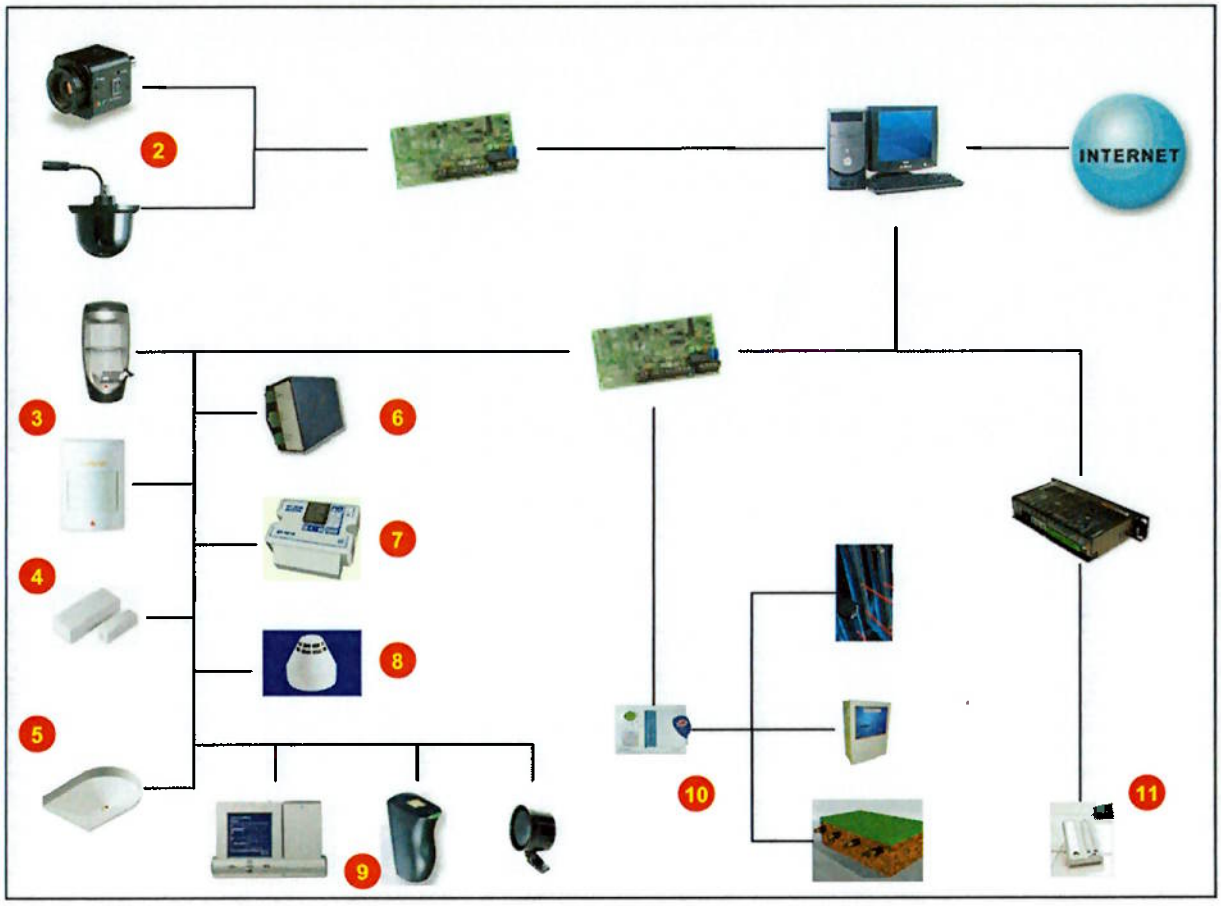


Figura 5.1 – Diagrama Estrutural do Sistema

A lista apresentada na Tabela 5.2 mostra os tipos de dispositivos que devem ser consideradas para compor o sistema de segurança. Ao lado do dispositivo, o número de associação com a Figura 5.1.

Tabela 5.2 – Lista Preliminar de Dispositivos

Dispositivo	**Função**
Câmera Externa (2)	Monitoração de áreas externas;
Câmera Interna (2)	Monitoração de áreas internas;
Sensor de Portas e Janelas (4)	Permitem detectar a abertura de portas e janelas;
Sensor de Impacto (5)	Permite detectar a violação ou pancada brusca na portas ou janelas;
Sensor de Movimento (3)	Permite detectar a movimentos em sua área de atuação

Sensor de fumaça (8)	Permite detectar focos de incêndio.
Sirene (9)	Emite sinal de alarme ou aviso quando acionado.
Central Eletrificadora (10)	Permite reagir com um choque caso ocorre tentativa de intrusão no perímetro da residência.
Cabo Microfônico (10)	Permite detectar a intrusão no perímetro da residência.
Leitor Biométrico (9)	Permite verificar a identidade de um usuário.
Teclado de controle (9)	Permite controle de todos os sistemas.
Controle de Luzes (11)	Permite controlar o acionamento de lâmpadas.
Módulo de Controle	Placas de Controle capazes de controlar um ou mais dispositivos.

Etapa 2 – Definição do sistema a ser modelado

O sistema deverá ser totalmente integrado. O conceito de integração de sistemas de segurança baseia-se no fornecimento de soluções completas e na premissa de que cada componente possa gerar ações nos demais componentes. Deste modo, procura-se fazer o gerenciamento da exceção, ou seja, gerenciam-se apenas os eventos mais críticos e que necessitem realmente da ação humana, deixando processos mecânicos e repetitivos para serem tratados de forma automatizada pelo sistema eletrônico [Cdiport, 2005].

Neste trabalho, considera-se o nível de interação de integração de sistemas, onde os múltiplos sub-sistemas são integrados por um único gerenciador. O sistema, como um todo, deve cumprir os pontos básicos de um sistema de segurança, e lidar com dois cenários, quando o usuário está em casa e quando não está [Bolzani, 2004].

O sistema de gerenciamento, da solução apresentada neste trabalho, concentra todas as funções de gerenciamento num micro-computador. Como estão sendo usados equipamentos de diferentes fabricantes, existe a necessidade de se integrar os softwares de gerenciamento de cada um deles.

De acordo com o projeto "DELTA Smart House 2005", da Universidade de Duke, a integração de softwares é possível mas é necessário desenvolver o software de integração.

Para o presente caso é considerado o software Elipse Scada para a criação de aplicativos de supervisão e controle. O Elipse Scada é ao mesmo tempo acessível, amigável e flexível. Este software foi concebido para uso em automação de processos. O Elipse Scada está disponível para as plataformas Microsoft Windows 95, 98, ME, NT, 2000 e XP [Elipse Software, 2005].

A seguir, detalham-se as relações objetivo-procedimento das funções que o sistema deve realizar.

Funções do nível primário de segurança

- Em situação de máxima segurança: para esta configuração todas as zonas da residência devem ser monitoradas e assume-se que não há qualquer morador presente;
- Em situação de média segurança: as zonas monitoradas devem ser definidas pelo morador, mas necessariamente serão as zonas, onde não deveria haver circulação de pessoas. Ex: jardineiro pode ir a casa fazer seu serviço sem ter acesso à parte interior da casa, desta maneira deve-se programar como uma zona a ser monitorada toda a área do quintal;
- Em situação de mínima segurança: somente a zona definida pelos limites do terreno é monitorada, considerando que os usuários circulam pela residência.

O nível primário de segurança define quais ações serão executadas, zonas monitoradas e quando cada ação poderá ser executada.

Funções do nível secundário de segurança

As funções podem envolver ações locais para sinalizar a ocorrência de perigo ao usuário ou podem ser ações externas para sinalizar através de meios de comunicação adequados os responsáveis pelo cuidado com a residência. A Tabela 5.3 abaixo exemplifica as ações que podem ser executadas:

Tabela 5.3 – Ações locais e externas

Ações locais	Ações externas
✓ Sirene ✓ Luzes	✓ Polícia ✓ Portaria ✓ Central de monitoriamento ✓ Comunicação por e-mail ✓ Comunicação por telefone ✓ Comunicação por sms, etc

As funções executadas de nível secundário são definidas de acordo com as situações identificadas no nível primário, podendo ser executadas individualmente ou em grupos.

Definição das zonas

As zonas, isto é, ambientes da residência, que devem ser objeto do sistema de segurança, podem ser definidas de modo a se sobreporem ou seguir uma relação de hierarquia através de ações e prioridades, de acordo com padrões e normas vigentes. A Figura 5.2 mostra a relação da definição de zonas com as funções de níveil primário e secundário de segurança.

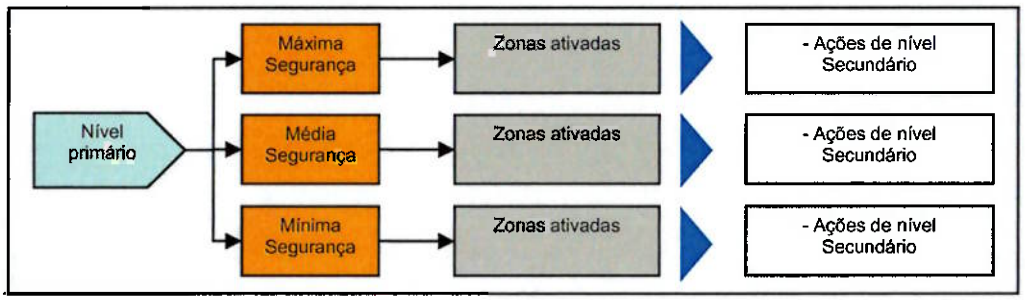


Figura 5.2 – Relacão entre as zonas e os níveis de segurança

A seguir, detalham-se os sub-sistemas de segurança considerados no presente caso.

1) Sub-sistema de vigilância com CFTV

A Figura 5.3 ilustra as funções consideradas para o sistema de vigilância com CFTV.

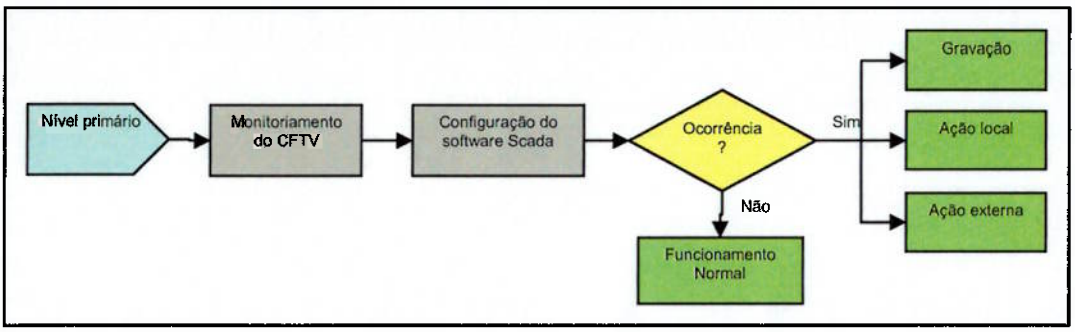


Figura 5.3 – Funções do sistema de vigilância com CFTV

2) Sistema de sensoriamento interno

O funcionamento dos sensores de presença, fundamentais para a detecção da presença de pessoas e integração de soluções. Como a residência é dividida em zonas, cada sensor ou sensores dedicados a uma zona estão associadas a pontos (locais) específicos. Este ponto identifica qual local foi, por exemplo, invadido por intrusos.

A Figura 5.4 ilustra as funções consideradas para o sistema de sensoriamento interno.

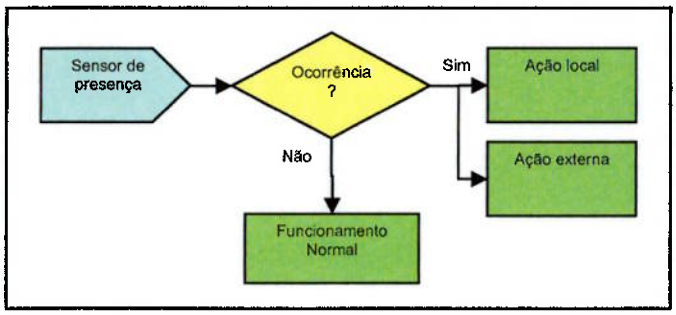


Figura 5.4 – Funções do sistema de sensoriamento interno

Neste exemplo de aplicação, o número de zonas será igual ao de sensores utilizados ou de ambiente da casa, o que facilita a identificação de um eventual sensor defeituoso ou com consecutivos disparos falsos.

3) Sistema de controle e automação de acesso

O sistema de controle e automação de acesso deve permitir aos usuários a restrição ou o acesso a residência e suas dependências através de dispositivos que conseguem identificar a pessoa, horário, dia que este foi identificado para o controle do fluxo das pessoas na residência autorizando somente aqueles que forem permitidos. Os dispositivos de controle de acesso são instalados nos portões e portas das residências. Este locais são escolhidos para assegurar uma maior segurança aos moradores. No presente caso considera-se a instalação de leitor biométrico.

A Figura 5.5 e Figura 5.6 ilustram as funções consideradas para o sistema de controle e automação de acesso.

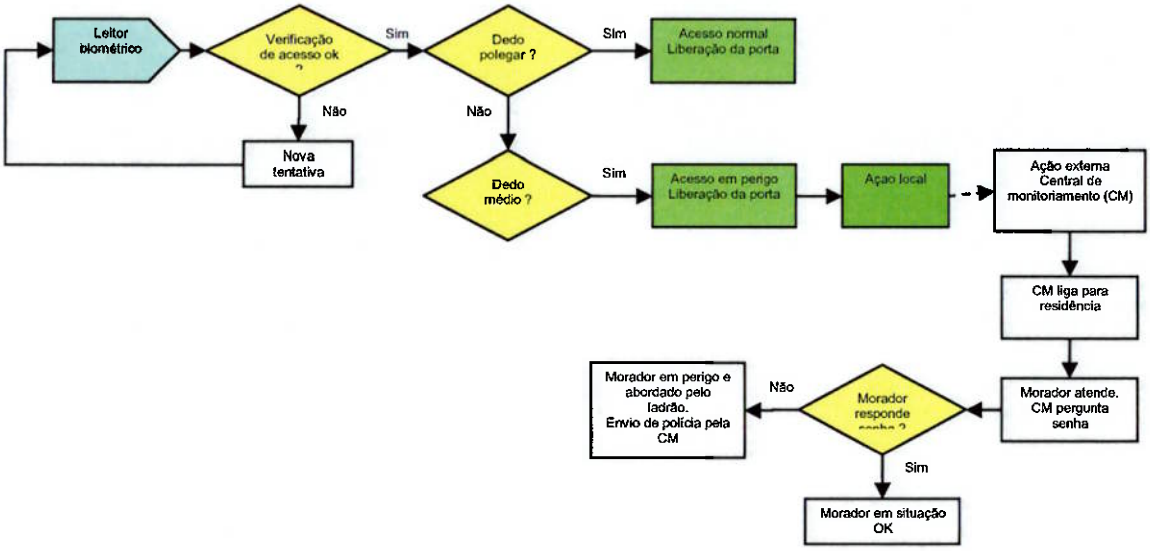


Figura 5.5 – Funções do leitor biométrico

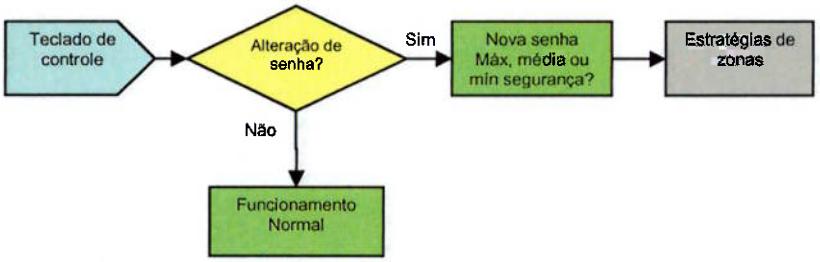


Figura 5.6 – Funções do teclado de controle

4) Sistema de detecção perimetral

O sistema de detecção perimetral envolve ações que protegem a residência contra a tentativa de intrusão pelos perímetros da residência, através de dispositivos de proteção. A cerca de infravermelho ativo (IVA) e a cerca eletrificada são instalados nos muros da residência de 3 metros. Considera-se ainda a instalação de um cabo microfônico interno ao muro para prevenir que ladrões tentem penetrar na residência por meio de um buraco no muro. A Figura 5.7 mostra onde são instalados as cercas e o cabo microfônico nos muros.

A Figura 5.8 e Figura 5.9 ilustram as funções consideradas para o sistema de detecção perimetral.

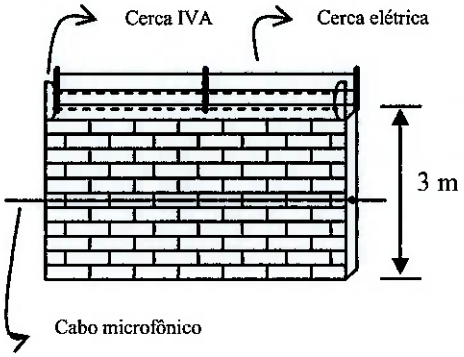


Figura 5.7 – Muro de proteção perimetral

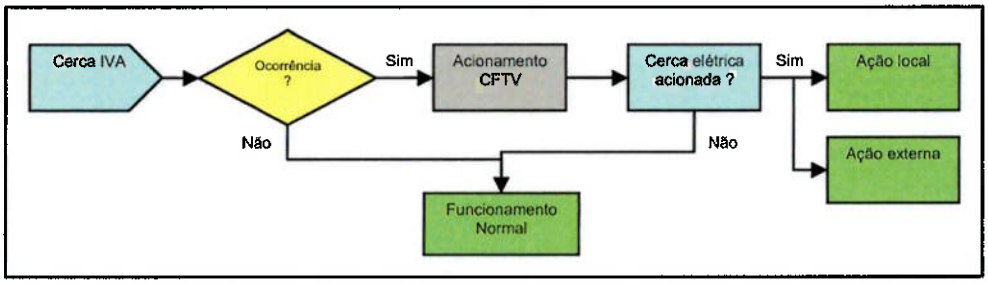


Figura 5.8 – Fluxo de Ação de Cercas de proteção perimetral

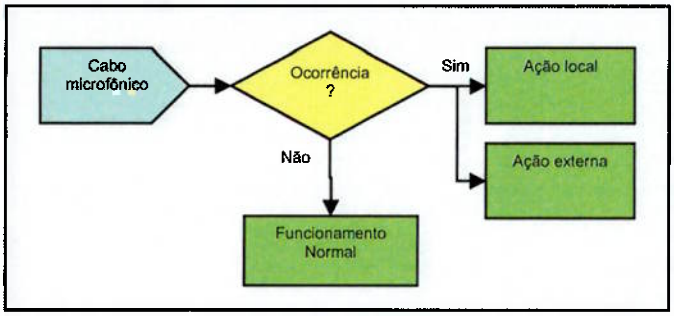


Figura 5.9 – Fluxo de Ação de cabo microfônico

A cerca IVA possui dois sensores ativos e dois passivos que fazem a detecção de qualquer variação no interrompimento do feixe. Normalmente em caso de queda de um galho de árvore, passagem de um pequeno objeto ou um pássaro pelo feixe, o tempo de interrupção é relativamente menor em relação à passagem de uma pessoa. Assim, estes não são caracterizados como uma ocorrência, evitando falsos alarmes.

A estratégia de utilizar duas cercas é para fornecer maior garantia quanto a proteção da residência, evitando possíveis invasões.

5) Sistema de alarmes

No caso de um usuário ser abordado por um intruso, existem alternativas que facilitam o aviso de emergência de modo silencioso, ou seja, sem que qualquer ação local seja acionada mostrando ao invasor que ações estão sendo tomadas. No presente caso considera-se o seguinte recurso:

- chaveiro com radio-frequência: este chaveiro utiliza um sistema de radio-frequência que fica ligado o sistema de alarmes. O morador, ao dispor de tal chaveiro, pode acionar um botão que faz o contato com o sistema de alarmes emitindo um sinal de pânico. O sistema de alarmes entra em contato com a central de monitoramento ou envio de sms aos outros moradores avisando sobre a ocorrência. Este chaveiro pode também ser utilizado por idosos no caso de ocorrência de acidentes, problemas de saúde, etc.

Dispositivos de Mercado Utilizados

Os dispositivos listados abaixo são os dispositivos de mercado escolhidos para constituir a solução que atende os requisitos e funções apresentadas acima. As características e especificações destes dispositivos estão apresentadas no Apêndice I.

Tabela 5.4 – Lista de dispositivos

Função	**Produto - Empresa**	**Comunicação**
Sistema de Vigilância		
Placa de Controle	GV-250 - Brubeki	Entrada: BNC X 4; DB15 X 2
Câmera Externa	WAT 207 - Brubeki	Saída: DB15
Câmera Interna	WAT 221S - Brubeki	Saída: DB15
Sistema de Alarme		
Placa de Controle	DGP-848 - Paradox	RS485; RS232
Sensor de Portas e Janelas	DGP2 - ZC1 - Paradox	RS485; RS232
Sensor de Impacto	456 - Paradox	RS485; RS232
Detecção de Movimento –Ambientes Externos	DG-85 – Paradox	RS485; RS232
Detecção de Movimento –Ambientes Internos	DG-55 – Paradox	RS485; RS232
Sensor de alagamento	Siemens	NA/NF
Sensor de fumaça	Siemens	RS 485; NA/NF
Sensor de vazam. de gás	Siemens	NA/NF
Sirene	MA-16 – X10	Liga / Desliga
Central Eletrificadora	Tornado - GHN	NA/NF
Cerca IVA	Newton - TSS	RS485,
Cabo microfônico	PMS/4 - TSS	NA/NF
Controle de Acesso		
Leitor Biométrico de Impressão Digital	CR-Vpass-A - Paradox	RS485
Teclado de controle	CR-R885-BL - Paradox	RS232, RS485, Wiegand

		IN/OUT
Sistema de Iluminação		
Controle de Luzes	TK134I – Smart Home	X10, RS485
Controle Remoto	HR12A – Smart Home	X10
Módulo de Controle	Quicklight - Home System	RS485, Saída: Ethernet

Etapa 3 – Modelagem estrutural do sistema

De acordo com os sub-sistemas selecionados e os dispositivos utilizados, pode-se decompor em sub-sistema de execução e coordenação. A Tabela 5.5 mostra esses dispositivos e sua classificação em comando, monitoração, atuação, detecção e realização.

Tabela 5.5 - Dispositivos usados no controle de sistemas de segurança

Classificação	Dispositivos
Dispositivos de Comando	Teclados, Painéis de Toque,
Dispositivo de Monitoração	Câmeras, Monitores, Leds,
Dispositivos de Atuação	Atuadores nas portas, solenóides,
Dispositivos de Detecção	Sensores de Presença, Sensores de Fumaça, Detectores
Dispositivos de Realização	PC

O modelo estrutural resultante é mostrado pela interação entre as diferentes partes do sistema, onde cada um dos elementos estruturais deste pode ainda ser dividido em módulos, para facilitar a modelagem do sistema. A Figura 5.10 mostra o modelo estrutural resultante.

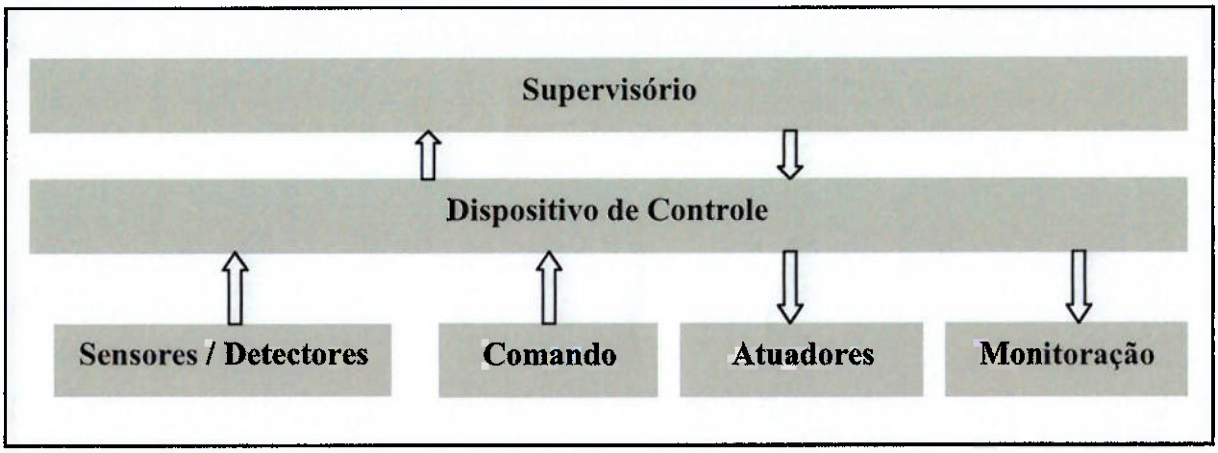


Figura 5.10 – Modelo Estrutural do Sistema

Etapa 4 - Modelagem conceitual e funcional do sistema de segurança

O modelo funcional do sistema de segurança é desenvolvido de acordo com as informações e a definição do sistema e segundo o modelo estrutural. Para a estruturação do modelo são utilizados o PFS, MFG e suas extensões.

Neste texto é apresentado o detalhamento de apenas algumas das atividades, levando-se em conta que a base do modelo do sistema segurança consiste nos detalhamentos apresentados, e que outras atividades do sistema são detalhados de modo análogo.

A Figura 5.11 abaixo mostra como são relacionadas todas as funções do supervisório, dispositivo de controle e os dispositivos de detecção, atuação, monitoração e comando.

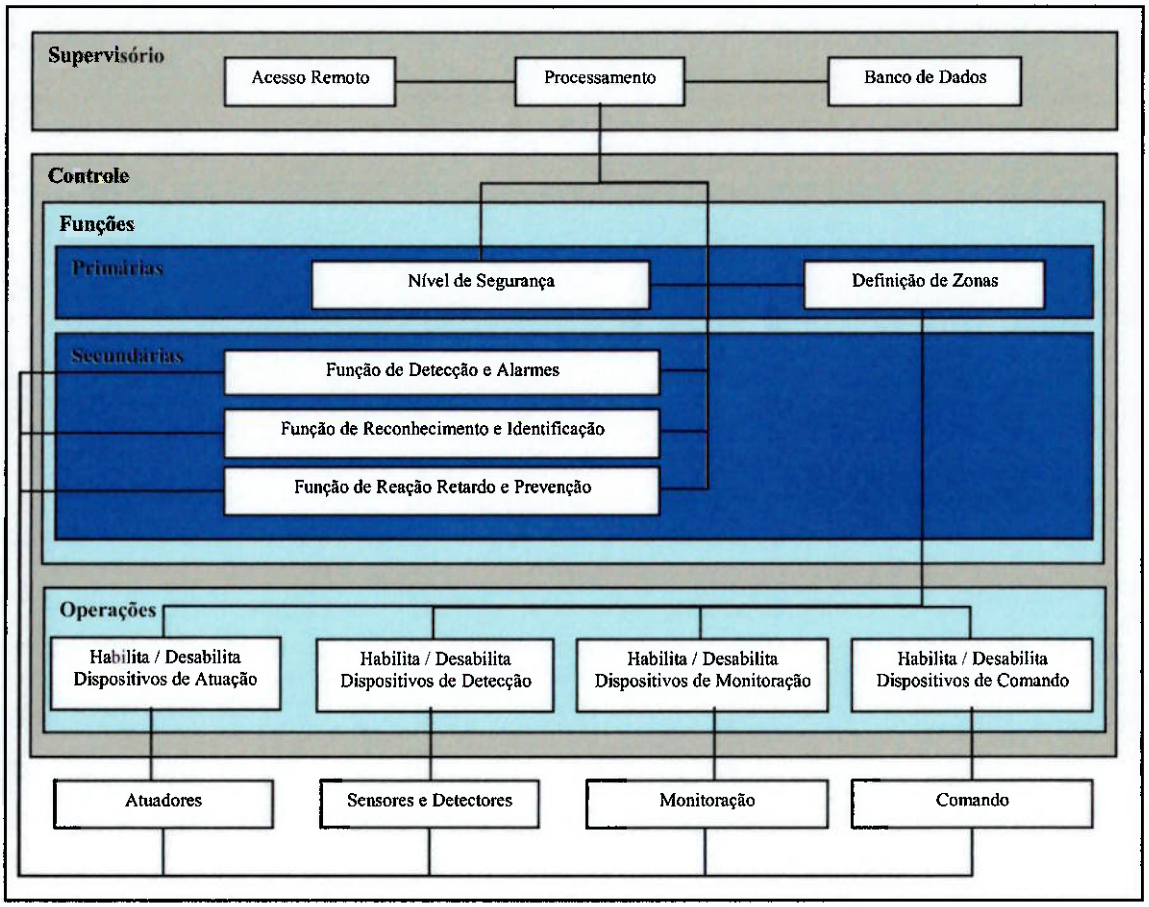


Figura 5.11 – Figura de relacionamento do sistema de segurança

Modelagem do sistema supervisório

O sistema supervisório envolve todas as funções que devem ser executadas no computador onde o sistema de segurança está implementado. É no sistema supervisório onde todas as decisões são tomadas através dos dados enviados pelos sub-sistemas de segurança.

O modelo apresentado para este sistema está na Figura 5.12 onde é divido em três partes principais, banco de dados, acesso remoto e processamento, que envolvem todas as funções executadas pelo software Scada.

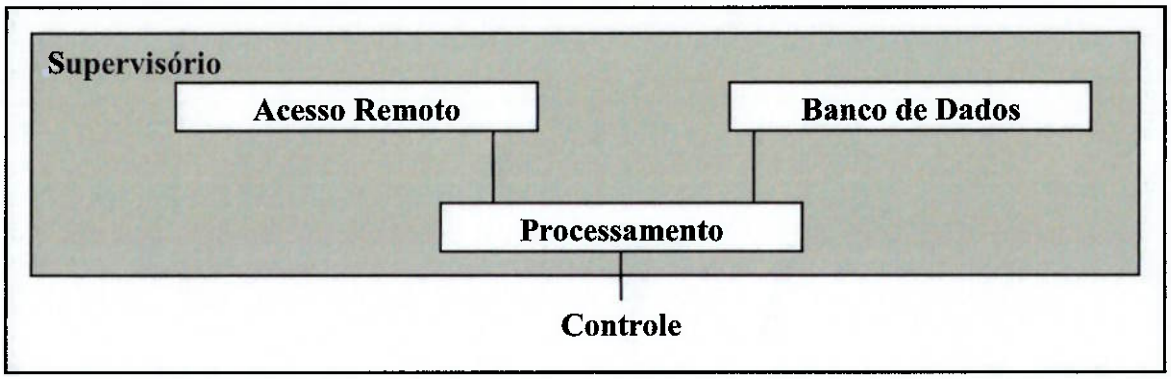


Figura 5.12 – Sistema supervisório

Modelagem do controle

O sistema de controle envolve as funções dos dispositivos controladores de cada sub-sistema de segurança. A Figura 5.13 apresenta o relacionamento entre as duas partes do controle onde as linhas que ligam os diferentes blocos, representam a existência de relação entre eles.

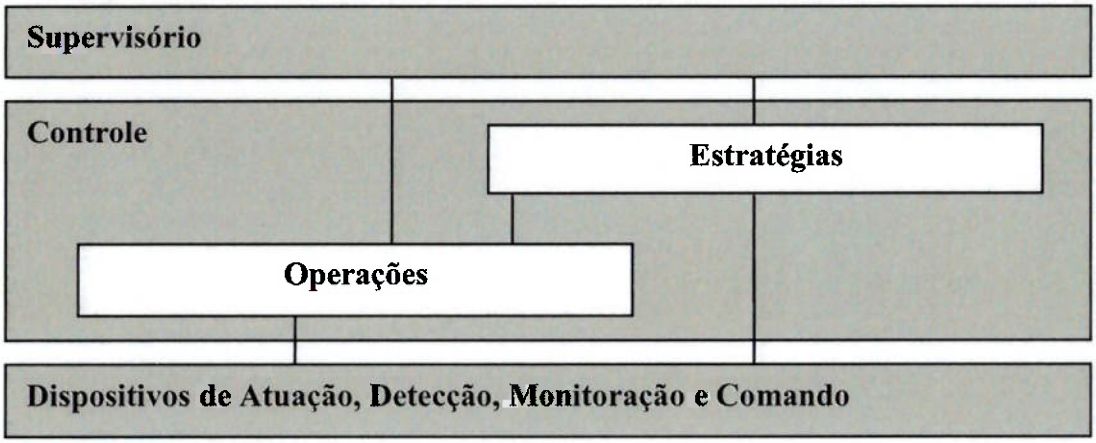


Figura 5.13 – Relacionamentos do controle

Modelagem de funções

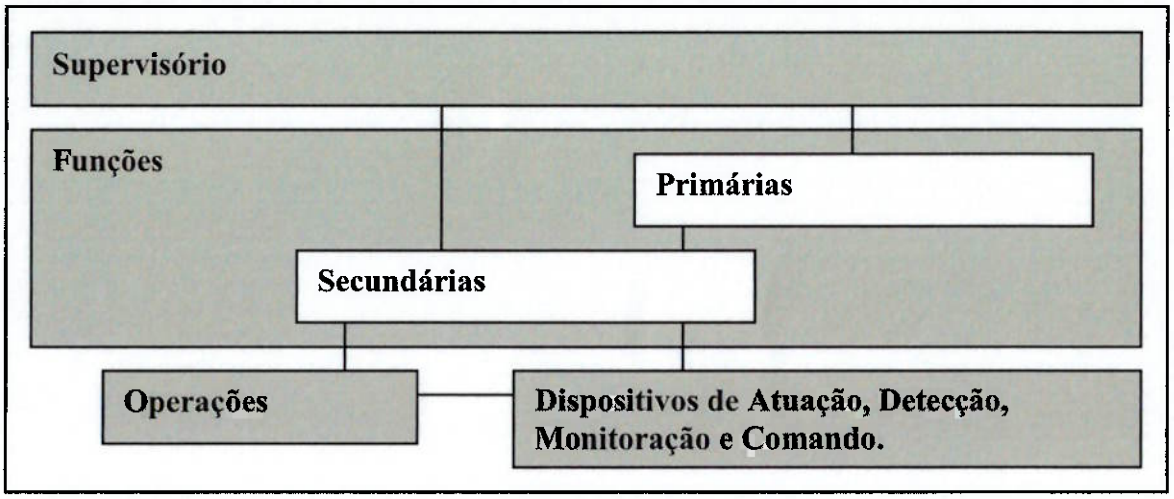


Figura 5.14 – Funções de nível primário e secundário

As funções estão separadas em dois grupos: primário e secundário. O grupo primário é aquela onde suas funções afetam a execução das funções do grupo secundário. As funções do grupo primário consideram o nível de segurança e a definição das zonas conforme mencionado na etapa 2. A Figura 5.15 mostra que a definição de zonas faz parte das funções de nível primário.

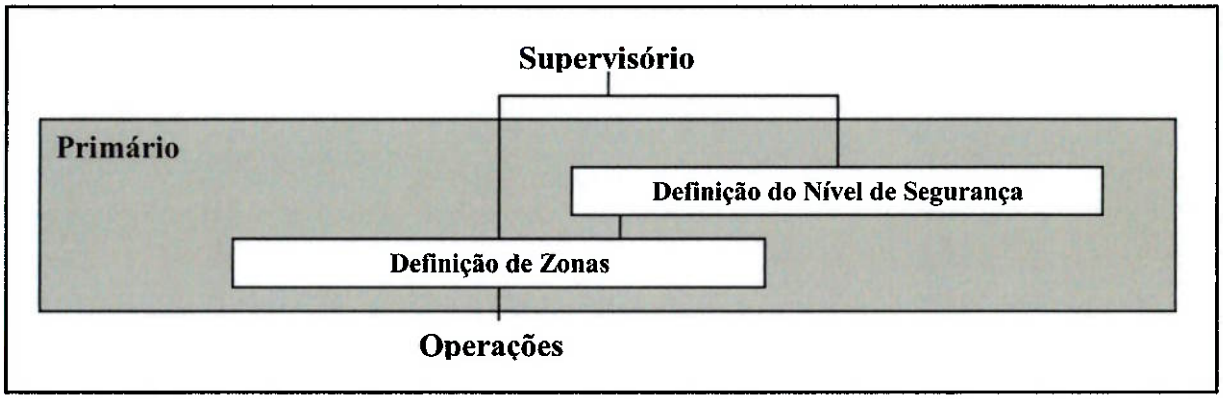


Figura 5.15 - Funções primárias

Definição do nível de segurança

A definição do nível de segurança envolve funções como ativar e desativar o respectivo nível de segurança. A Figura 5.16 modela este processo.

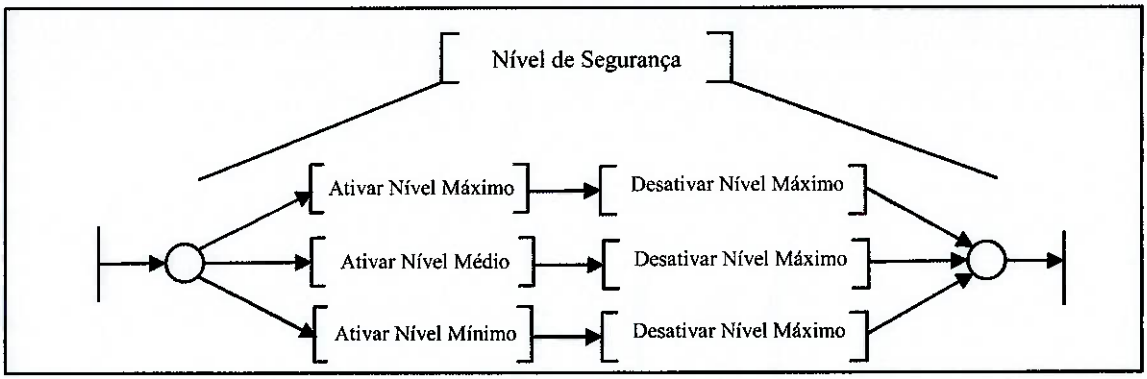


Figura 5.16 – PFS das funções associadasao nível de segurança

O detalhamento em MFG das funções associadas ao nível de segurança é apresentado na Figura 5.17.

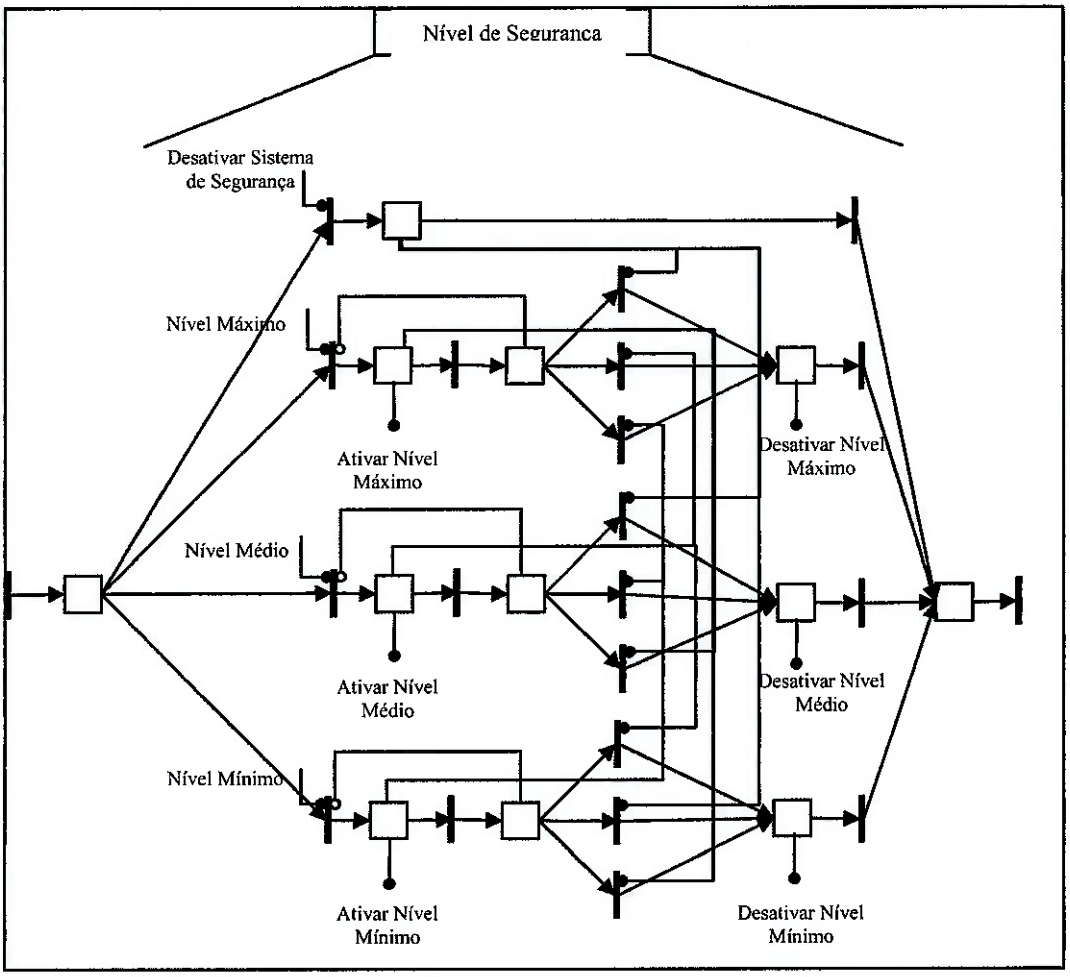


Figura 5.17 – MFG das funções associadas ao nível de segurança

Os sinais relacionados com a ativação/desativação do nível máximo, médio, mínimo do sistema de segurança vêm do supervisório, onde são tomadas as decisões. Em qualquer situação, apenas um nível de segurança pode estar ativo, por essa razão a ativação de um modo automaticamente desabilita os outros.

Estratégias de Zoneamento

A estratégia de definição das zonas está diretamente ligado a atividade de habilitar ou desabilitar os diferentes dispositivos de segurança para cada nível de segurança. A Figura 5.18 ilustra o PFS deste processo.

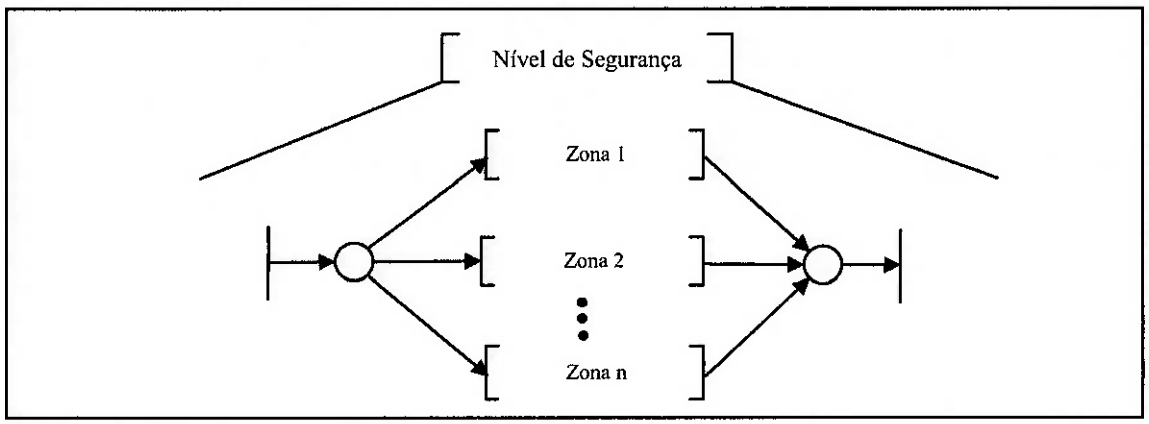


Figura 5.18 – PFS das funções associadas a estratégias de definição das zonas

Os dispositivos podem pertencer a uma ou mais zonas de segurança, podendo ou não serem habilitados ou desabilitados conforme o nível de segurança. O MFG na Figura 5.19 detalha este processo.

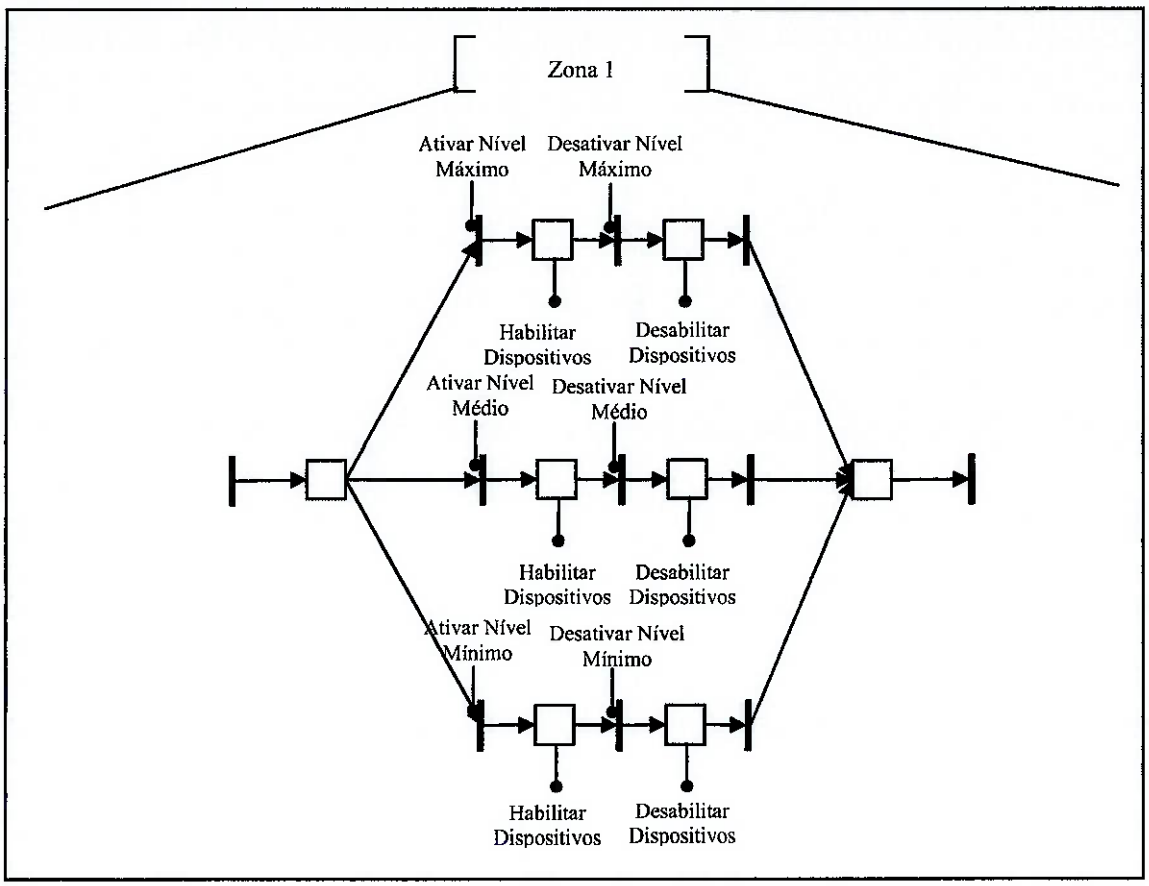


Figura 5.19 – MFG da funções associadas a estratégias de definição das zonas

Funções de nível secundário

O grupo secundário é composto por funções onde suas ações dependem do grupo primário. As funções do grupo secundário são (Figura 5.20):

- funções de detecção e alarmes;
- funções de reconhecimento ou identificação;
- funções de prevenção ou dissuasão, reação e retardo.

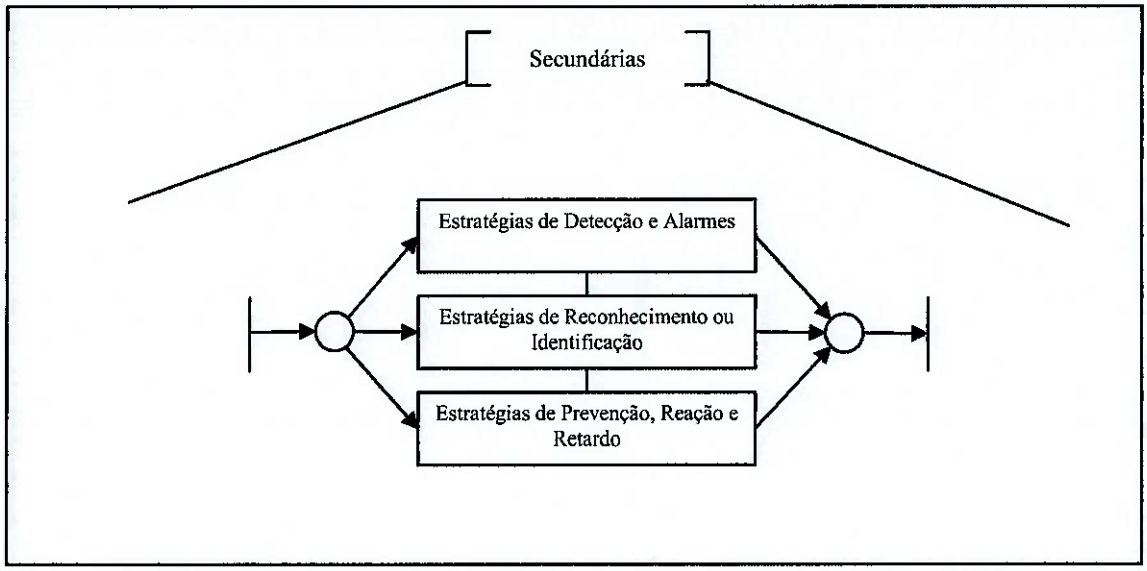


Figura 5.20 - MFG das funções de nível secundário

Funções de reconhecimento e identificação

As funções de reconhecimento e identificação são acionadas pelos respectivos dispositivos: leitor biométrico e teclado de controle. A Figura 5.21 detalha este processo.

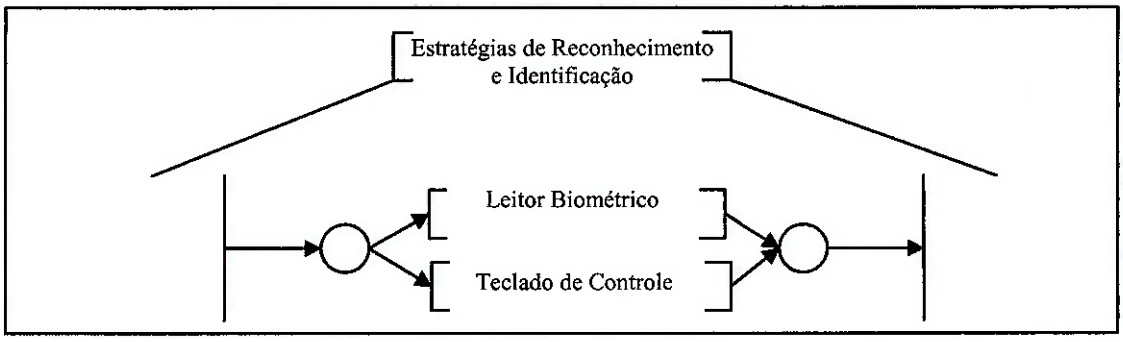


Figura 5.21 – PFS das funções de reconhecimento e identificação

A função de reconhecimento e identificação, tanto para leitor biométrico como para o teclado de controle, possuem a mesma estrutura de operação. Desta maneira será apresentado apenas o modelo funcional do leitor biométrico.

Quando existe um sinal de requisição de acesso, a função de reconhecimento e identificação é acionada. Esta função verifica com o banco de dados do supervisório se a senha é correta, incorreta ou se é senha de pânico. Caso a senha seja incorreta, e esta seja carregada três vezes seguidas é negado a passagem e executa-se uma ação externa, como enviar um sms ao morador e avisar a central de segurança da possível tentativa de invasão. Caso a senha seja uma senha de pânico, é liberada a passagem e são executados ações externas, enviando um sms avisando a central de segurança de problema de invasão. Caso a senha seja correta, é liberada a passagem e o sistema volta ao seu estado inicial. A Figura 5.22 ilustra o MFG deste processo.

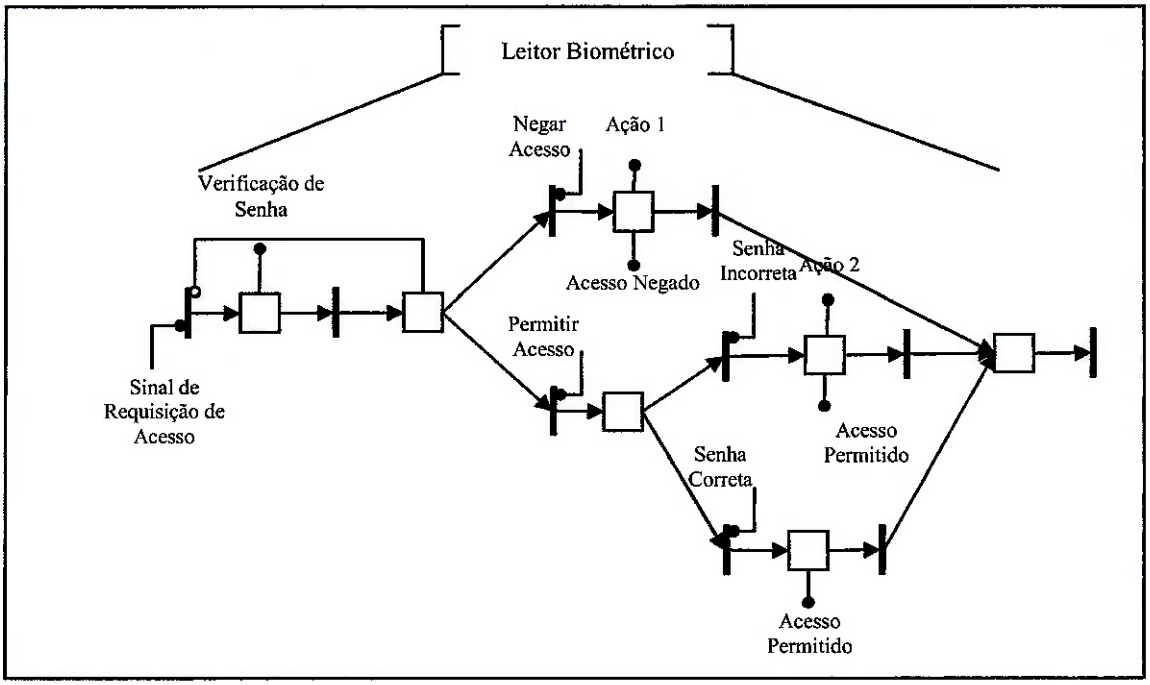


Figura 5.22 - MFG das funções de reconhecimento e identificação para leitor biométrico.

Função de reação e retardo

As funções de reação e retardo são utilizadas toda vez que um sinal de perturbação ocorrer. As Figuras 5.23, 5.24, 5.25, 5.26 ilustram o PFS/MFG de parte deste processo.

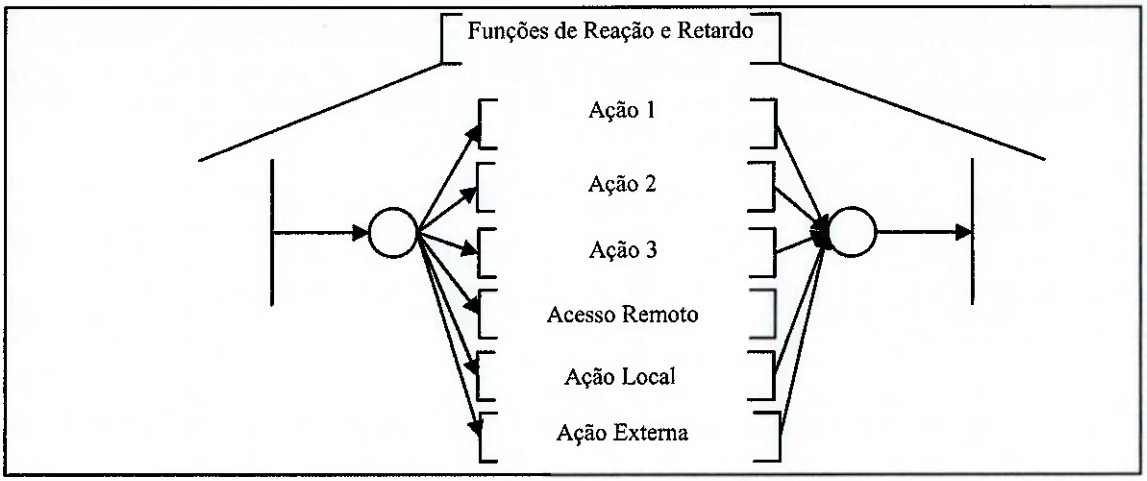


Figura 5.23 - PFS das funções de reação e retardo.

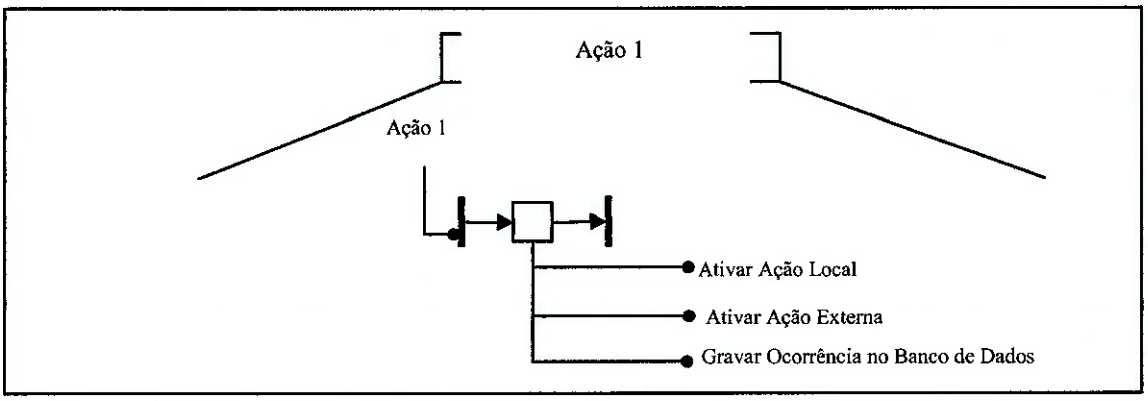


Figura 5.24 - MFG da ação 1

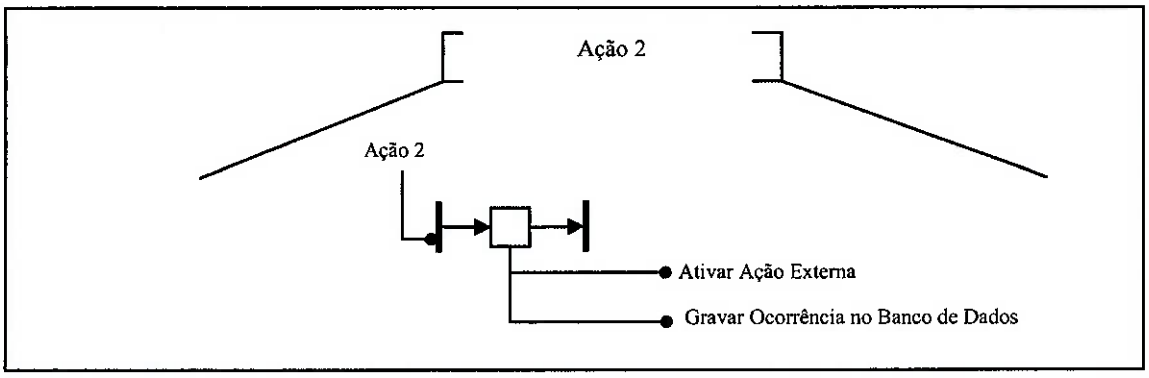


Figura 5.25 - MFG da ação 2

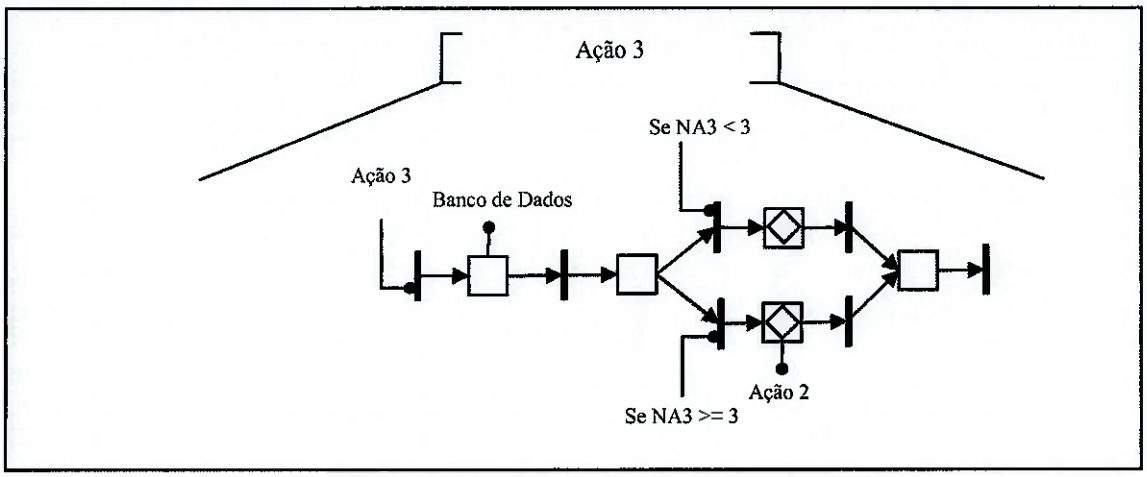


Figura 5.26 - MFG da ação 3

As ações locais são todas as atividades de reação e retardo que podem ser executadas no local sem a necessidade de comunicação externa (Figura 5.27).

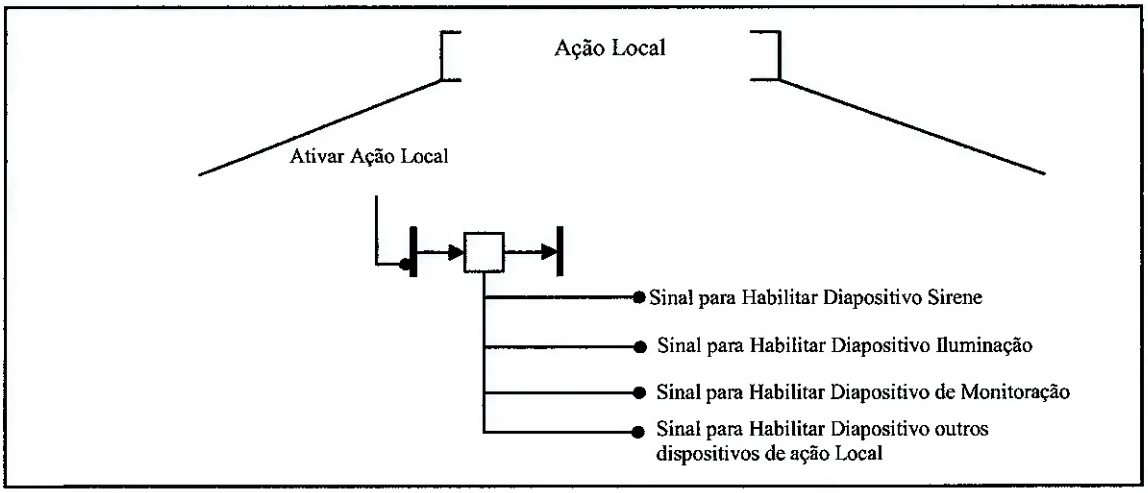


Figura 5.27 - MFG da ação local

A Figura 5.28 ilustra o MFG do processo associada a ação externa.

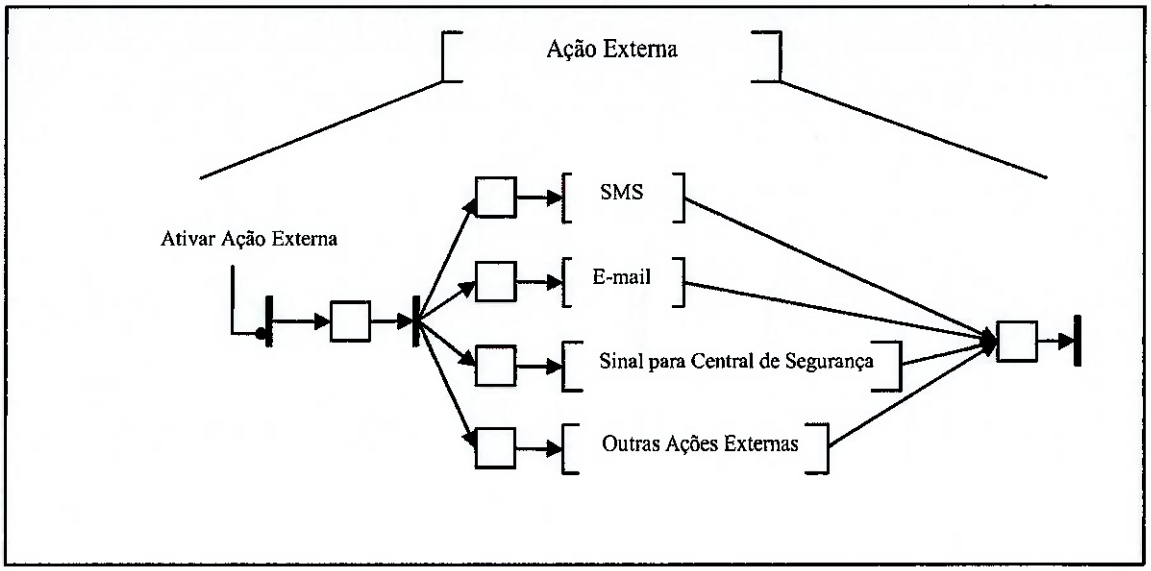


Figura 5.28 - MFG da ação externa

Modelagem de operações

As operações são as funções básicas de controle dos dispositivos. A Figura 5.29 ilustra a estrutura destas funções.

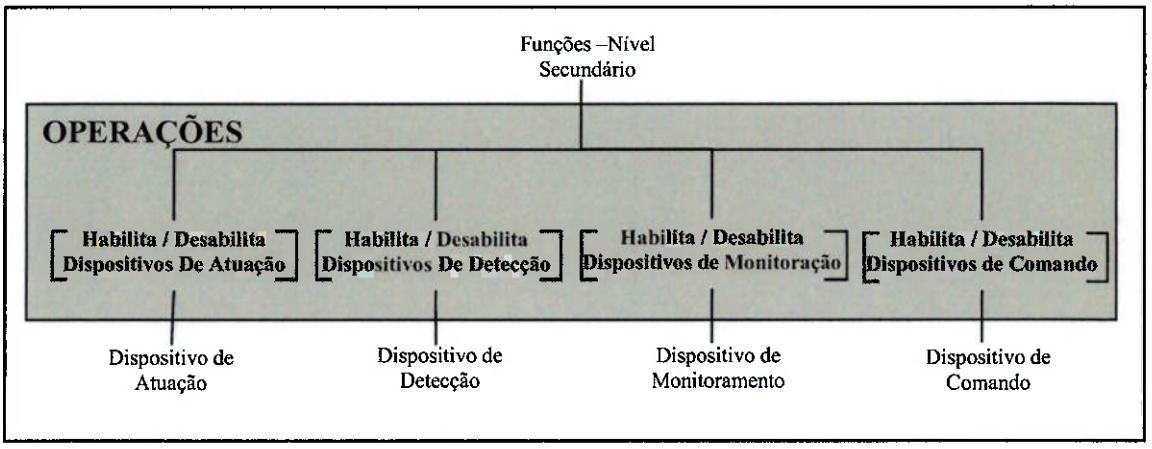


Figura 5.29 – Estrutura das operações

A modelagem das funções de controle para os dispositivos de atuação está na Figura 5.30.

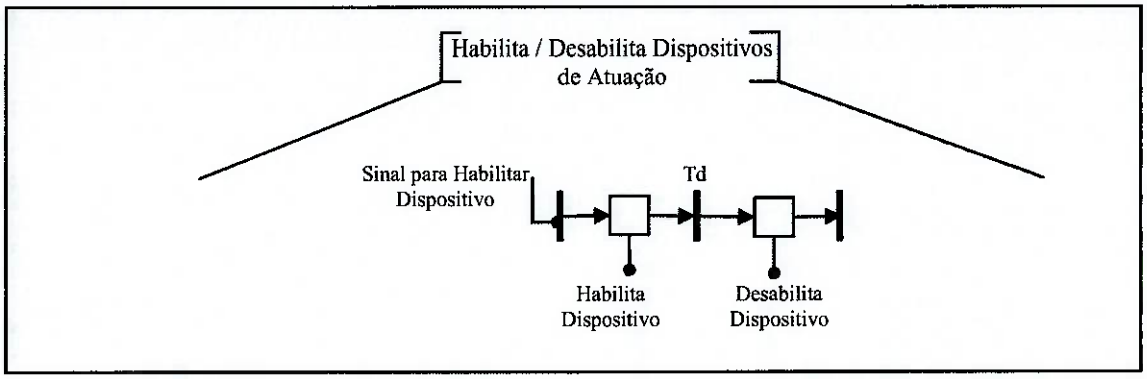


Figura 5.30 – MFG das funções de operação dos dispositivos de atuação

A modelagem das funções de controle para os dispositivos de detecção está na Figura 5.31.

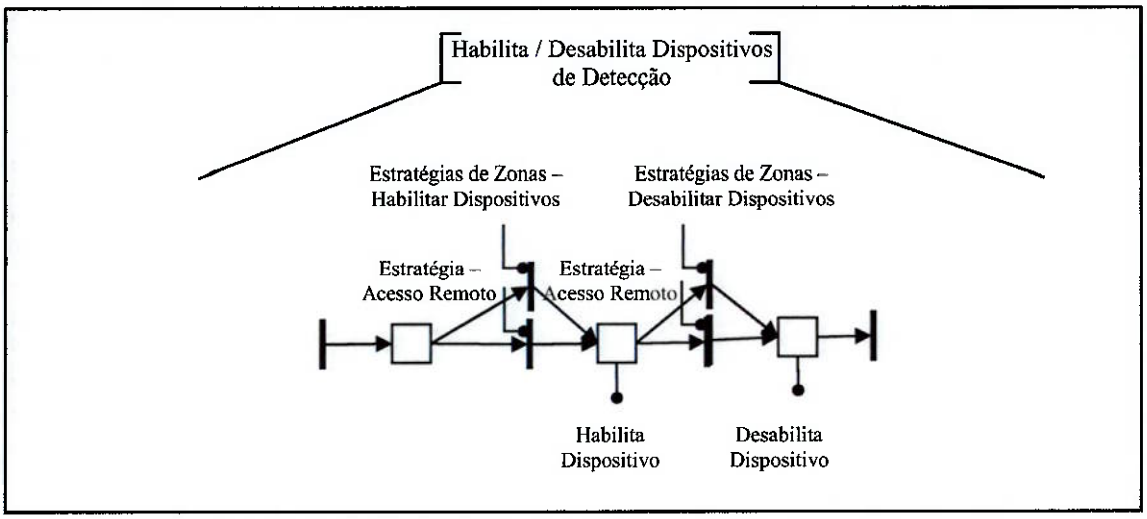


Figura 5.31 – MFG das funções de operação dos dispositivos de detecção

A estrutura das funções de controle para os dispositivos de monitoração está na Figura 5.32.

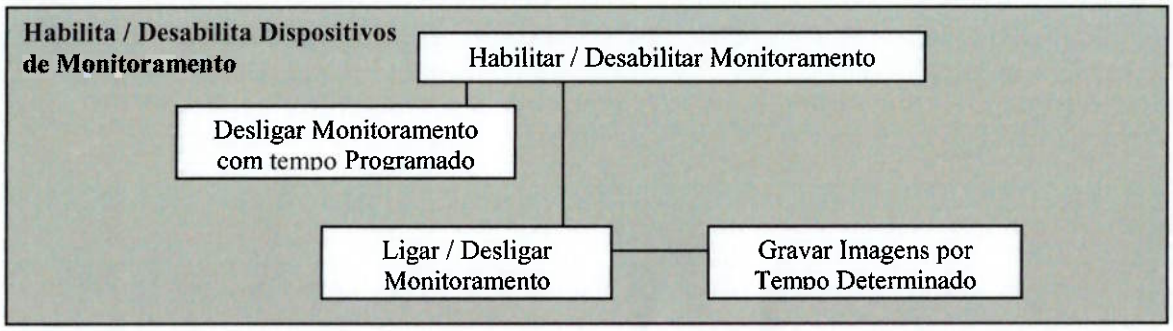


Figura 5.32 – Estrutura das operações dos dispositivos de monitoração

O controle dos dispositivos de monitoração deve ligar e desligar as câmeras e o gravador conforme necessidade, verificar a detecção de movimento pelas imagens enviadas pela câmera e requerer uma ação devida. A Figura 5.33 ilustra o PFS deste processo e a Figura 5.34 detalha as atividades em MFG.

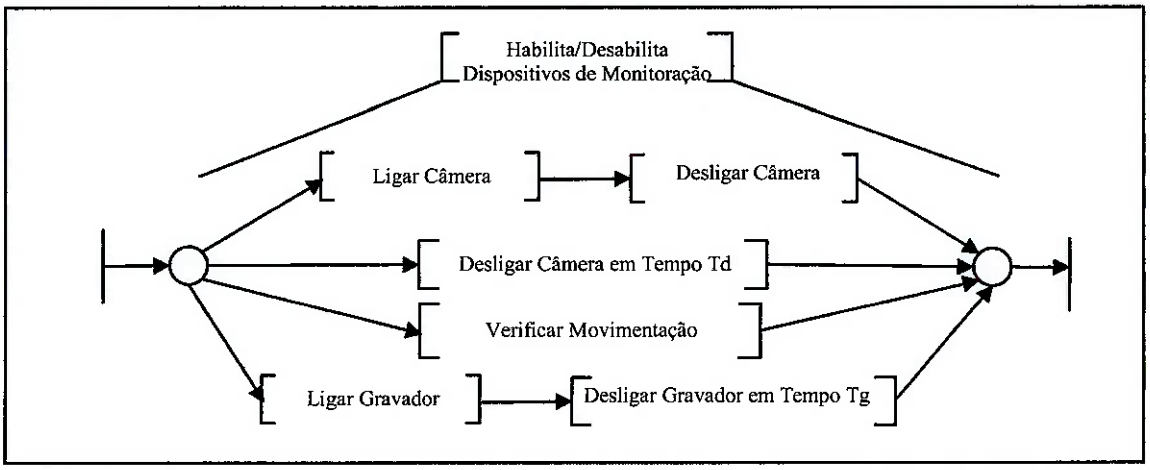


Figura 5.33 – PFS das operações dos dispositivos de monitoração

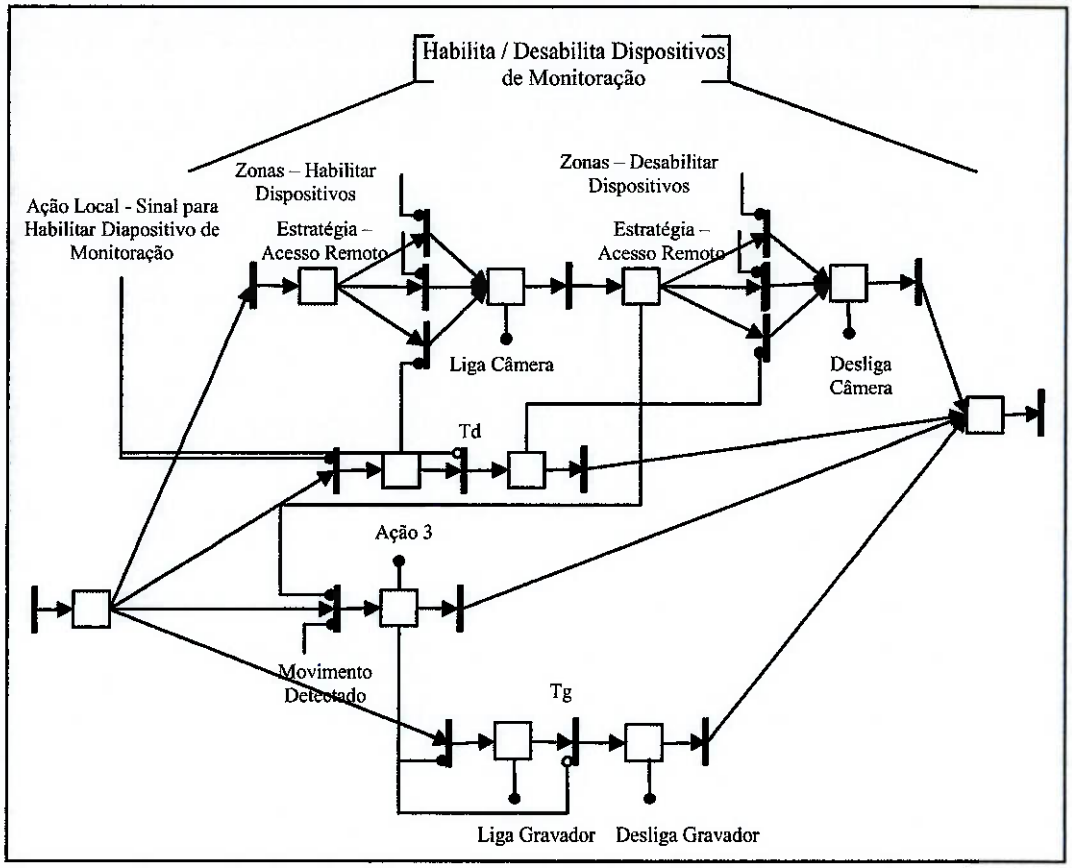


Figura 5.34 – MFG das operações dos dispositivos de monitoração

Pelo fato dos dispositivos de comando já possuírem certas funções de controle no próprio dispositivo, as atividades de habilitar e desabilitar os dispositivos de comando são simples e estão apresentadas na Figura 5.35.

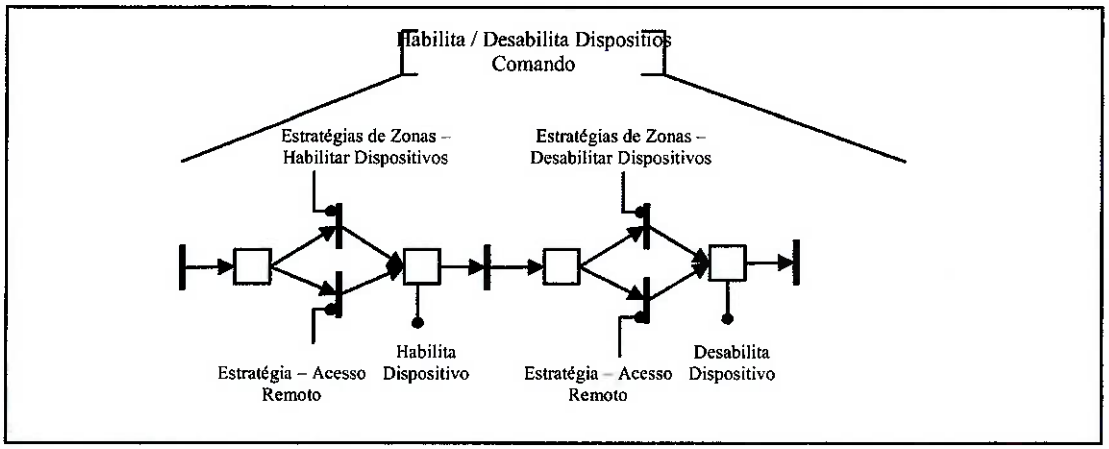


Figura 5.35 – MFG das operações dos dispositivos de comando

Modelagem dos dispositivos de detecção, controle, atuação e comando

O modelo do dispositivo de detecção é apresentado na Figura 5.36. Todo e qualquer tipo de sensor utilizado no sistema de segurança proposto pode ser modelado desta maneira.

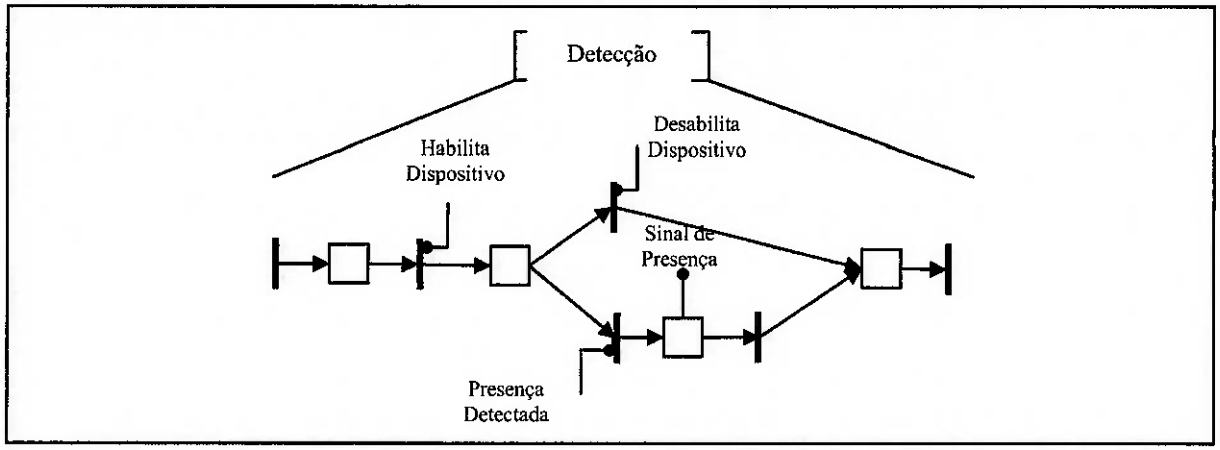


Figura 5.36 – MFG de dispositivo de detecção

O modelo em MFG da sirene (dispositivo de monitoração) é apresentado na Figura 5.37.

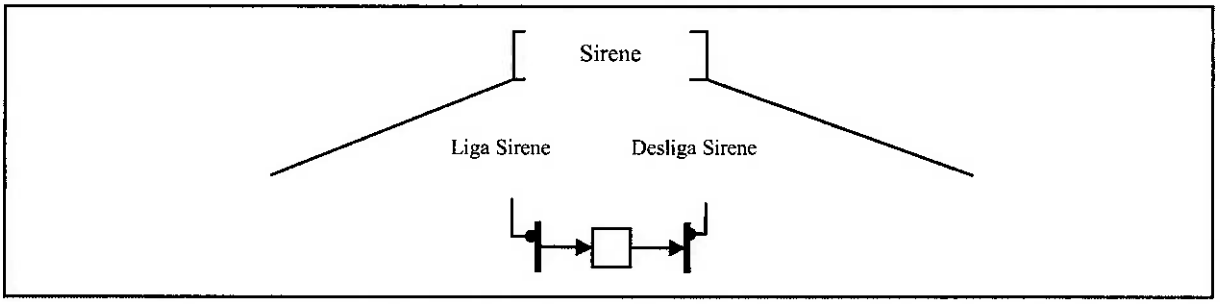


Figura 5.37 – MFG da operação da sirene

O modelo em MFG de dispositivos de iluminação (dispositivo de atuação) é apresentado na Figura 5.38.

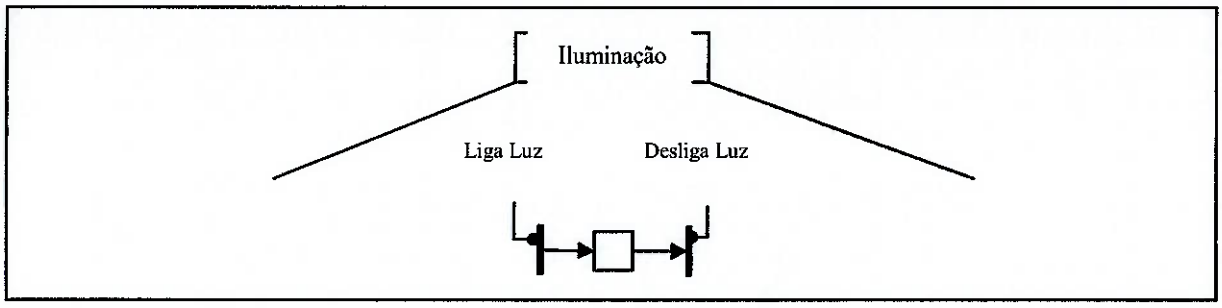


Figura 5.38 – MFG de dispositivos de iluminação

O dispositivo de monitoração é formado pelo grupo de câmeras e gravador de imagem (Figura 5.39).

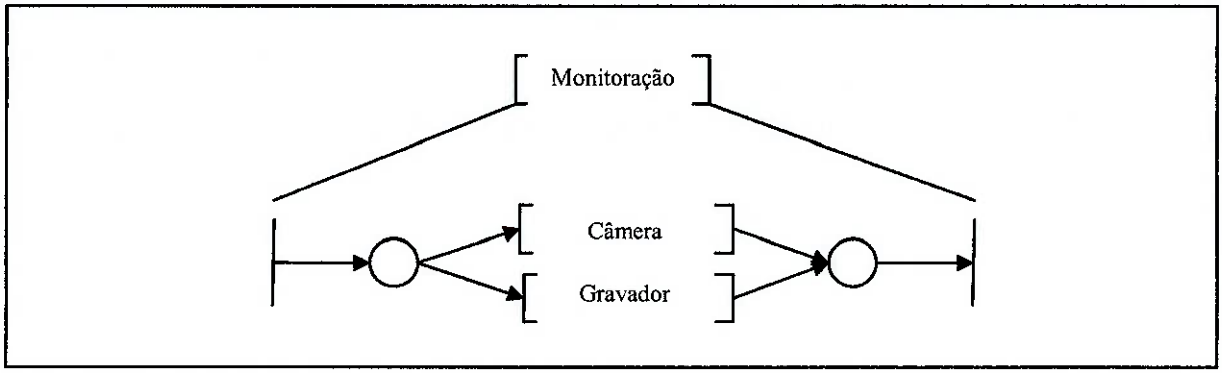


Figura 5.39– PFS do dispositivo de monitoração

O modelo em MFG dos dispositivos de monitoração é apresentado na Figura 5.40.

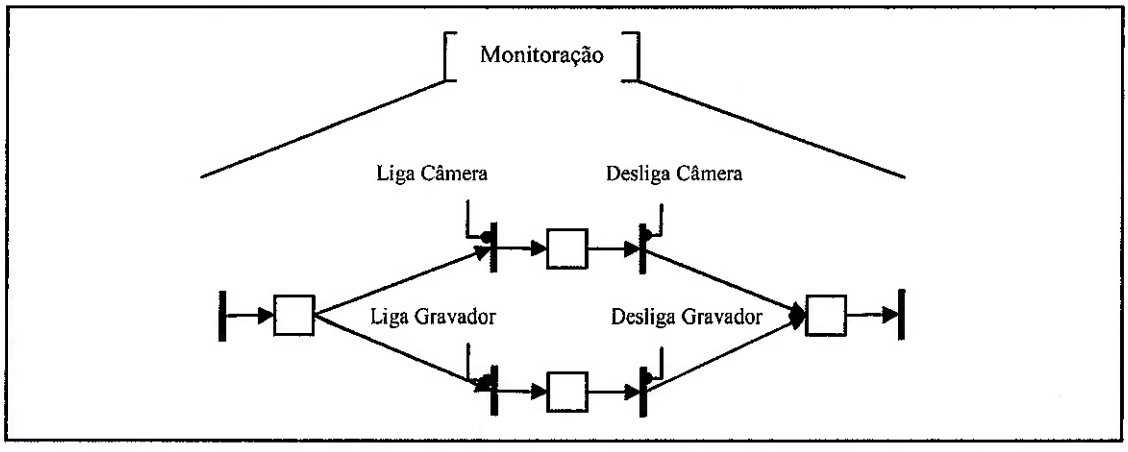


Figura 5.40– MFG do dispositivo de monitoração

O modelo do dispositivo de comando é um pouco mais complexo devido às funções envolvidas. O dispositivo comando modelado está associado ao sub-sistema de controle de acesso, que deve verificar a requisição de acesso e permitir ou barrar o acesso conforme resposta do sistema de operações.

O modelo em PFS dos dispositivos de controle de acesso é apresentado na Figura 5.41 e o detalhamento em MFG está na Figura 5.42.

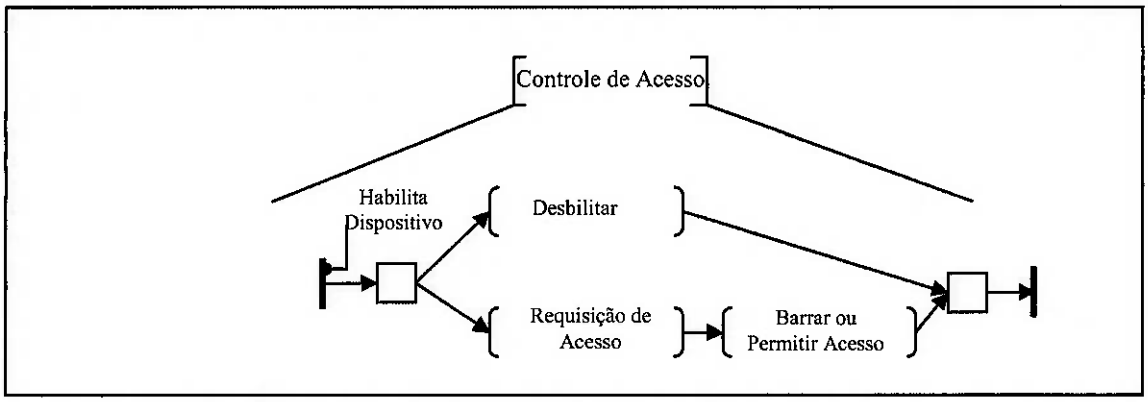


Figura 5.41 – PFS do dispositivo de controle de acesso

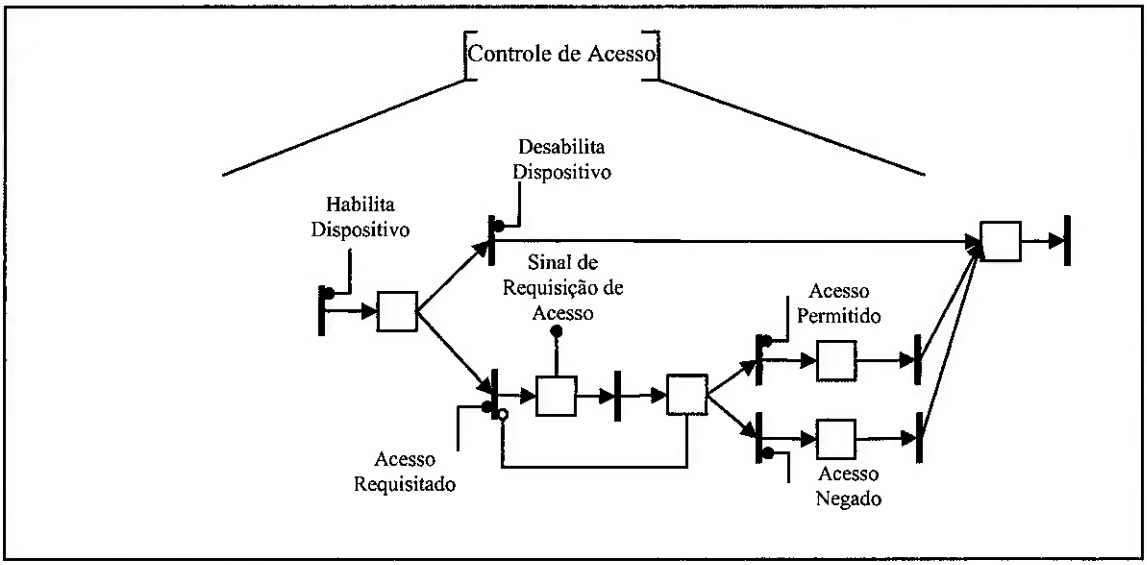


Figura 5.42 – MFG do dispositivo de controle de acesso

5.2. Observações finais do capítulo

Neste capítulo foi verificada a efetividade da metodologia para modelar o sistema de segurança para automação residencial. A aplicação desta técnica permitiu a modelagem do sistema de segurança passo a passo a partir do levantamento das informações do sistema. Assim, foram desenvolvidos os modelos do sistema iniciando com um modelo estrutural de todo o sistema, para depois derivar os modelos conceituais em PFS refinando-os em modelo funcionais em MFG (que inclui o MFG original e suas extensões).

Verificou-se que a aplicação da metodologia de modelagem facilita a construção do modelo detalhado do sistema de segurança residencial, servindo assim de auxílio ao projeto e definição de diretrizes para tornar o sistema de segurança parte da residência inteligente, no qual um controle adequado apresente resultados muito mais satisfatórios.

CAPÍTULO 6

RESULTADOS E CONCLUSÕES

Este trabalho desenvolve a modelagem de sistema de segurança para automação residencial através da abordagem de sistemas a eventos discretos, e mediante o uso da rede de Petri. Uma metodologia é adotada para o desenvolvimento estruturado de modelos e proporcionar sua interpretação, facilitando o processo de análise e o aprimoramento da especificação do sistema.

A metodologia aplicada considera modelos conceituais e funcionais, cuja finalidade é facilitar a construção de um modelo global do sistema de segurança considerando sua integração com outros subsistemas residenciais, além de, disponibilizar um suporte adequado à flexibilidade do sistema e permitir sua utilização em uma posterior etapa de implementação do sistema.

O exemplo de aplicação confirmou a utilidade e eficiência da rede de Petri e do PFS/MFG para modelagem de sistemas de segurança para automação residencial. Demonstrando-se assim a possibilidade de se utilizar o PFS/MFG para apoio ao projeto (modelagem, análise e especificação) de residências inteligentes.

Verificou-se que o PFS/MFG através do modelo funcional resultante é efetivo para definir as funções de controle, facilitando desta forma a implementação do controle e a integração do sistema de segurança com outros subsistemas.

A metodologia aplicada no presente trabalho apresenta as seguintes características:

- estabelece uma forma sistemática para a abordagem do sistema de segurança e a construção de seus modelos, os quais podem ser usados para a verificação do sistema e sua implementação;
- descreve as características e operações do sistema de modo claro e uniforme;
- descreve o sistema do nível conceitual ao detalhado de acordo com a estrutura hierárquica das atividades do sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

ALARMWOLX. Disponível em: <http://www.alarmwolx.com.br>. Acesso em: 05 agosto 2005.

AMADO, I. **Biometria "do futuro" já é realidade no Brasil.** Disponível em: <http://www.ilheusamado.com.br>. Acesso em: 05 agosto 2005.

ARAKAKI, J. **Análise de Sistemas de Manufatura Através da Metodologia MFG/PFS e Regras de Produção.** São Paulo, 1993. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo.

ARAKAKI, J. et al. **Aplicação da Metodologia PFS/MFG na Modelagem de Sistemas de Edifícios Inteligentes In: WORKSHOP SINTED SOBRE EDIFÍCIOS INTELIGENTES,** Resumenes, Varadero, Cuba, 1998, p.98-100.

ASSOCIAÇÃO BRASILEIRA DE AUTOMAÇÃO RESIDENCIAL. **Peculiaridades dos Sistemas de Automação Residencial.** Disponível em: <http://www.aureside.org.br>. Acesso em: 22 março 2005.

BOLZANI, C. **Residências Inteligentes.** Editora Livraria da Física, 2004.

BRUBEKI. **Serviços e Equipamentos**. Disponível em: <http://www.brubeki.com.br>. Acesso em: 05 agosto 2005.

CONFIHASTES. **Fabrica de hastes para cerca elétrica**. Disponível em: <http://www.confihaste.net>. Acesso em: 05 agosto 2005.

Cury, J.E.R., Torrico, C.R.C., Cunha, A.E.C. **A New Approach for Supervisory Control of Discrete Event Systems**. European Control Conference, 2001.

DOROMO. **Solução Completa – Conforto e Segurança em seu Lar** – Disponível em: <http://www.doromo.com.br>. Acesso em: 08 julho 2005.

DUKE UNIVERSITY. **Home Automation**. Disponível em: <http://delta.pratt.duke.edu/projects>. Acesso em: 05 agosto 2005.

ELIPSE SOFTWARE. **Supervisão e Controle de Processos com Mais Resultados.** Disponível em: <http://www.elipse.com.br>. Acesso em: 15 setembro 2005.

FINGERSEC. **Sobre Biometria**. Disponível em: <http://www.fingersec.com.br>. Acesso em: 05 agosto 2005.

FINLEY, M. **Survey of Intelligent Buildings Concepts**. IEEE Communications Magazine. April, 1991. p.18-23.

FUTURE HOUSE. **Automação e Segurança**. Disponível em: <http://www.futurehouse.com.br>. Acesso em: 22 março 2005.

GHN ELETRÔNICA. **Sistemas Eletrônicos de Segurança**. Disponível em: <http://www.ghneletronica.com.br>. Acesso em: 05 agosto, 2005.

GLOBAL SYSTEM. **Sistemas contra incêndio**. Disponível em: <http://www.globalsyst.com.br>. Acesso em: 05 agosto 2005.

GUSTIN, G. D. B. **Aplicação de Redes de Petri Interpretadas na Modelagem de Sistemas de Elevadores em Edifícios Inteligentes.** São Paulo, 1999. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo.

HASEGAWA, K.; TAKAHASHI, K.; MIYAGI, P. E. **Application of the Mark Flow Graph to Represent discrete Event Production Systems and System Control.** Transactions of the Society of Instrument and Control Engineers. v.24, n.1, p.67-75, 1988.

HASEGAWA, K. **Modeling, Control and Deadlock Avoidance of FMS, In**: Conferências Plenárias, XI CBA, São Paulo, SBA, 1996, p.37-51.

HO, Y. **Discrete Event Dynamic Systems. Analyzing Complexity and Performance in the Modern World, IEEE Control Systems Society**, Sponsor New York, 1991.

KAGOHARA, M. Y. **Aplicação da Metodologia PFS/MFG a Sistemas de Produção Enxuta (Lean Manufacturing Systems).** São Paulo, 1998. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo.

KRONER, W. M. **An intelligent and responsive architecture; In**: Automation in Construction, p. 381-393, vol. 6 n.5 September 1997.

LIU, W. **Aplicação da Metodologia MFG/PFS no Desenvolvimento de Sistemas de Informações de Indústrias de Manufatura.** São Paulo, 1993. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo.

MIYAGI, P. E. **Control System Design, Programming and Implementation for Discrete Event Production System by Using Mark Flow Graph.** Tóquio, Japão, 1988. Tese (Doutorado) – Tokyo Institute of Technology.

MIYAGI, P. E. **Controle Programável – Fundamentos do Controle de Sistemas a Eventos Discretos.** Editora Edgard Bluncher, São Paulo, 1996.

MURATA, T. Petri nets: properties, analysis and applications. Proceedings of IEEE, v. 77, n.4, p. 541-580, April, 1989.

NETO, J. S. C. **Edifícios de alta tecnologia.** Editora Carthago & Forta, 1994.

OLIVEIRA, H.; OLIVEIRA, T. **Controlador de Acessos Modular Baseado em Tecnologia de Cartões de Proximidade.** Tese (Graduação) – Escola Superior de Tecnologia, Setubal, 2004.

PARADOX. **Security Systems**. Disponível em: <http://www.paradox.ca> . Acesso em: 05 agosto 2005.

PRACTER. Disponível em: <http://www.practer.com.br>. Acesso em: 05 agosto 2005.

PROCAD AUTOMAÇÃO INDUSTRIAL. **Scada Software**. Disponível em: <http://www.scada.com.br>. Acesso em: 05 agosto 2005.

PRODUTEK. **Segurança eletrônica**. Disponível em: <http://www2.produtek.com.br>. Acesso em: 05 agosto 2005.

PERES, M. P. **Guia do CFTV - Curso Básico.** Dezembro, 2004

PETERSON, J. L. **Petri Net Theory and the Modeling of Systems.** Prentice-Hall, N.J., 1981

REISIG, W. **A Primer in Petri Net Design.** Springer-Verlag, Berlin Heidelberg, Alemanha, 1992.

RESELLER WEB. **Soluções em Smart Card**. Disponível em: <http://www.resellerweb.com.br>. Acesso em: 05 agosto 2005.

SANTOS Fo, D. **Proposta do Mark Flow Graph estendido para a Modelagem e Controle de Sistemas Integrados de Manufatura.** São Paulo, 1993. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo.

SILVA, M. **Las Redes de Petri: en la Automática y la Informática.** Madrid, Editorial AC, 1985.

SILVA, J. R.; MIYAGI, P. E. A formal Approach to PFS/MFG: **A Petri net representation of discrete manufacturing systems, Studies in Informatics and Control**, v.5, n.2, 1996.

SILVA, J. R.; MIYAGI, P. E.: PFS/MFG: **A High Level Net for the Modeling of Discrete Manufacturing Systems. Balanced Automation Systems – Architectures and design methods.** p. 349-362. Camarinha-Matos, L. M. e Afsarmanesh, H. (eds), Grã-Bretanha, 1995.

SUGISAWA, M. **A Study and Modeling Deadlock Avoidance for Discrete Production Systems with Shared Resources**. Tóquio, 1998. Tese (Doutorado) – Tohin Yokohama University.

TUCANO. **Comércio de Alarmes e Sistemas Eletrônicos**. Disponível em: <http://www.tucano2.com.br>. Acesso em: 05 agosto 2005.

X10. **Home Solutions**. Disponível em: <http://www.x10.com.br>. Acesso em: 05 agosto 2005.

ZURAWSKI, R.; ZHOU, M. **Petri nets and industrial applications: a tutorial.** IEEE Transactions on Industrial Electronics, v.41, n.6, p.567 – 583, December, 1994

APÊNDICE I

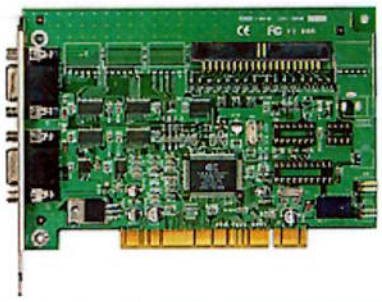
É apresentada, nesta parte do trabalho, as características e especificações dos dispositivos escolhidos para o estudo de caso considerado.

Sistema de Vigilância com CFTV

Entre os vários tipos de CFTV existentes no mercado, é utilizado o sistema de CFTV digital da Brubeki [Brubeki, 2005] que tem como componentes os itens abaixo:

- Processador: Placa controladora, para instalação em micro-computadores, capaz de controlar até 16 diferentes câmeras.

Tabela I.1. – Especificações da Placa de Controle GV - 250

GV- 250	
 Error!	
Especificações	
Tipos de Entrada	GV-250 BNC: BNC X 4
	GV-250 D-Type: DB15 X 2
Entrada(s) de Vídeo	4, 8, 16 Câmeras
Entrada(s) de Áudio	1 canal
Taxa de Gravação	15 fps (NTSC), 25fps (PAL).
Taxa de Exibição	15 fps (NTSC), 25fps (PAL).
Resolução de Vídeo	320x240, 640x240, 640x480, 640x480 S/W
Formato de Compressão	Wavelet, MPEG-4, GeoMPEG-4
Suporte a GV-DSP	Sim
Suporte a GV-A16	Sim

Suporte a GV-NET/IO Card	Sim
Dimensões	GV-250 BNC: 132mm x 100mm
	GV-250 D-Type: 132mm x 100mm
Nota: Atualmente o GV-250 não é compatível com placas-mãe com chipset VIA.	
Requisitos de Sistema	
Sistema Operacional	Windows 2000 / Windows XP
CPU	Pentium III 500 (mínimo)
RAM	256MB (mínimo)
HD	40 GB (recomendado)
Placa de Vídeo	nVIDIA GeForce2 MX200 32MB

- Câmeras Internas e Externas

Para este trabalho utilizou-se câmeras da WATEC WAT207-CD [Brubeki,2005] que são compatíveis com a placa de controle da Brubeki.

Tabela I.2. – Especificações da câmera externa da WATEC

WAT 207 CD Color

- Sensor de imagem: 1/4
- Pixels: 290K PAL, 250K NTSC
- Resolução horizontal: 320 linhas de TV
- Iluminação mínima: 3 lux F2.0 com microlente de 3.8 mm
- Visão Angular (HV): 51° (H) x 40° (V)
- Função de balanço branco: Automático
- Íris eletrônica
- Velocidade do shutter: PAL ON: 1/50~1/100,000 seg.(automático), OFF: 1/50 seg. NTSC ON: 1/60~1/100,000 seg. (automático), OFF: 1/60 seg.
- Alimentação: DC+6.0V ~+7.5V(Aprox. 260 mA)
- Peso: Aprox. 145g (incluindo cabo e receptor WAT-300 RX)
- Adaptador: WAT-AD603 incluso

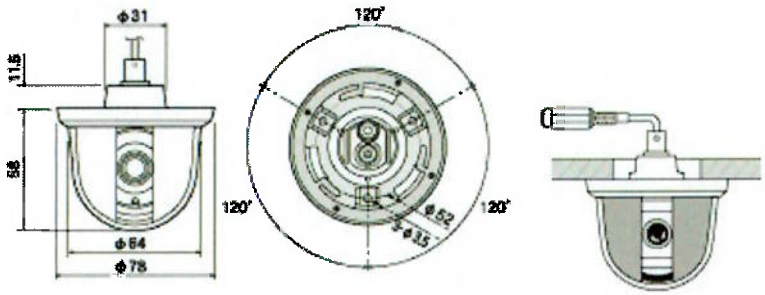


Figura I.1. – Dimensões da câmera WAT207-CD

Tabela I.3. – Especificações da Câmera interna da WATEC

WAT – 221S

- Sensor de imagem: CCD1/2"
- Tamanho da célula: NTSC: 8.4 μ m (H) x 9.8μ m (V)
- N° total de pixels: NTSC: 811(H) x 508 (V)
- N° de pixels efetivos: NTSC: 768 (H) x 494 (V)
- Sincronização interna
- Sistema de scaneamento: 2:1 interlaçado
- Saída de vídeo: composto, 1 Vp-p, 75 ohm
- Saída de vídeo: Y/C (Y Íris sync, C Croma Burst)
- Nível de vídeo: 100 IRE/75 IRE selecionável
- Resolução: 450 linhas de TV (vídeo comp.) /480 linhas e TV (Y/C)
- Iluminação mínima: 0.1 lux. F 1.2 (AGC High)
- Correção de Gamma= 0.45 (ON) / 1.0 (OFF)
- AGC ON= 8~36dB (High), 8~24dB (Low) /OFF=8dB
- Ruído S/N: 50dB (AGC OFF)
- Modo AE: OFF, FL. (1/100), 1/250, 1/500, 1/1000, 1/2000, 1/4000, 1/10000 sec. EL: OFF (1/60 ~ 1/1000 sec.)
EL: FL (1/100 ~ 1/10000 sec.)
- Compensação de luz de fundo ON/OFF selecionável
- Balanço do branco: Auto, Present: 6300K, 5100K, 4200K, 3200K, PQB, L, MWB
- Montagem de Lentes: CS/ C
- Íris automática: Vídeo/ DC drive selecionável
- Alimentação: DC 10.8 ~ 13.2V (12V ± 10%)
- Corrente Max: 190mA
- Temperatura de operação: -10° ~ +40°C
- Temperatura de armazenamento: -30° ~ +70°C

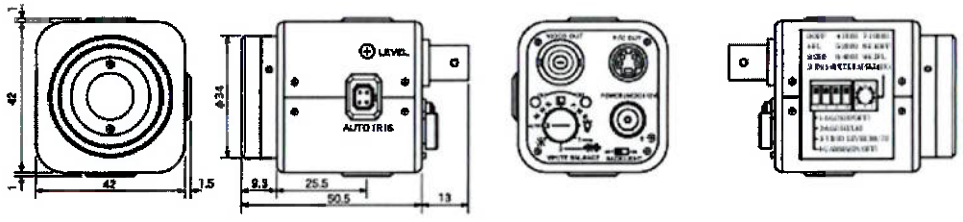


Figura I.2– Dimensões da Câmera WAT-221S

Sistema de Alarme

Dentre os vários tipos de sensores de portas e janelas existentes no mercado, foi utilizado o sensor DGP2-ZC1 [Paradox, 2004] conforme mostra a Figura I.3:

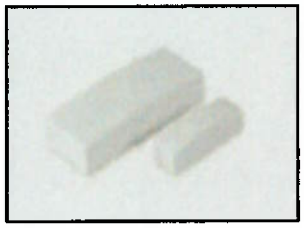


Figura I.3. – Sensor magnético para portas e janelas

Especificações:

Consumo máximo de corrente de 14mA;

- Tamanho: 74mm x 20mm x 30,5mm;
- Temporizador de 1 a 3 minutos;
- 1 zona de configuração;

Dentre os vários tipos de sensores de impacto existentes no mercado, foi utilizado o sensor 456 [Paradox, 2004] conforme mostra a Figura I.4:

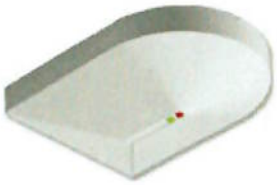


Figura I.4. – Sensor de Impacto

Especificações:

- Análise de todo espectro de áudio e infrasonico;
- 7 filtros digitais de freqüências e amplificador digital de ganho e freqüência;
- Análise de onde de choque e impacto;
- Alta imunidade de sinais RFI e EMI;
- Sensibilidade ajustável: cobre até 9m quando está ajustado com alta sensibilidade e até 4.5m quando ajustado para baixa sensibilidade;

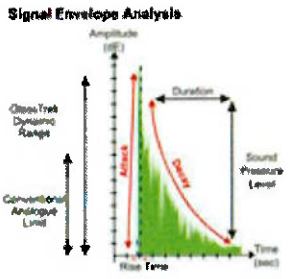


Figura I.5.– Espectro de Sinal

No presente trabalho, foram utilizados os sensores infravermelhos ativos como o modelo de detecção de movimento digital Digigard DG-85 (Figura I.6) para o ambiente externo da residência e o modelo Digigard DG-55 (Figura I.7) para o ambiente interno.

Figura I.6. – Sensor digigard DG-85

Especificações:

- Lentes protegidas dos raios ultra-violeta;
- Temperatura de operação de -35° a 50°C;
- Sistema de filtro *dual optical*;
- Imunidade a animais menores que 40kg;
- Ajuste de sensibilidade multi-nível;
- Visão de 11m x 11m;
- Ângulo de 90°;
- Máxima corrente de 30mA;
- Características comuns a todos os sensores de detecção de movimento;
- Dois modos de operação

Figura I.7. – Sensor digigard DG-55

Especificações:

- Sensor *dual;*
- Visão de 12m x 12m;
- Ângulo de 110°;
- Características comuns a todos os sensores de detecção de movimento;
- Máxima corrente de 15mA;
- Rejeição de 10V/m de 10MHz a 1GHz; 2.1m a 2.7m;

Figura I.8 – Eletrificador para cercas Tornado

Especificações:

- Configuração do modo de disparo: temporizado ou sob-demanda;
- Ajuste de sensibilidade;
- 3 setores: 1 da cerca, 1 com fio e 1 sem fio*;
- Memória de setor atuado: adverte o usuário quanto à existência de algum disparo;
- Indica os 6 últimos os 6 (seis) últimos setores que causaram algum disparo na central*.
- Ignora um setor que disparar a central 3 (três) vezes consecutivas;
- Programação dos tempos de entrada, saída e duração do disparo;
- 2 Saídas independentes: sirene de 12 Volts e contatos NA/NF (10A máx.).
- Saída de 8.000 ou 10.000 Volts;
- Entrada para sensores com/sem fio;
- Dimensões: 235 x 170 x 73 milímetros

o recurso só existe se o módulo recepetor estiver conectado à central.

Sistema de controle e automação de acesso

Exemplo de leitor biométrico de impressão digital que foi utilizado neste trabalho é o leitor biométrico da paradox, CR-VPass-A.

Figura I.9 – Leitor Biométrico

Especificações:

Dimensões	Altura: 130mm (5.12.) Largura: 50mm (1.97.) Profundidade: 65.5mm (2.5.)
Comunicações:	RS232, RS485, Wiegand IN/OUT
Tempo de processamento:	< 3 segundos
Tempo de Identificação Falsa:	< 1 segundo para 100 usuários
Taxa de Aceitamento (FAR):	1.0%
Taxa de falsa Rejeição (FRR):	1.0%
Tensão:	7V to 24Vdc

Figura I.10 – Leitor de Cartão de Proximidade e Senha

Especificações:

Dimensões	Altura: 130mm (5.12.) Largura: 50mm (1.97.) Profundidade: 65.5mm (2.5.)
Comunicações:	RS232, RS485, Wiegand IN/OUT
Tempo de processamento:	< 1 segundos
Tempo de Identificação Falsa:	< 1 segundo para 100 usuários
Taxa de falsa Rejeição (FRR):	5.0%
Tensão:	7V to 24Vdc

Sistema de Iluminação

No presente trabalho é utilizado o sistema X-10, como o controle de ligar/desligar lâmpadas (Figura I.11), controle remoto (Figura I.12) e temporizador (Figura I.13).

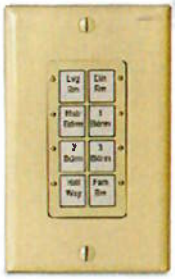


Figura I.11 - Controle de ligar/desligar luzes TK134I

Especificações:

- Comunicação powerline 2-ways;
- Recebe confirmação de status;
- Programação fácil;
- Controle de 8 diferentes cômodos;
- 120 KHz, mínimo 6V pico a pico a 5 ohm.

Figura I.12 - Controle remoto HR12A

Especificações:

- Sistema de controle remoto wireless;
- Botões de intensidade de luz;
- Controle de ventiladores, stereos, lâmpadas etc;
- Alcance de 100 pés.

Figura I.13. - Timer 2-way X-10 23883TW

Especificações:

- Inclui temporizador de contagem regressiva;
- Comunicações em 2 vias asseguram que as luzes apaguem como requerido;
- Compatível com X-10;
- Fácil de ajustar para períodos longos;
- Barra de 8 leds que mostram o nível de brilho;