JORGE RADY DE ALMEIDA JUNIOR

SEGURANÇA EM SISTEMAS CRÍTICOS E EM SISTEMAS DE INFORMAÇÃO – UM ESTUDO COMPARATIVO

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Professor Livre Docente, junto ao Departamento de Engenharia de Computação e Sistemas Digitais

São Paulo
2003

JORGE RADY DE ALMEIDA JUNIOR

SEGURANÇA EM SISTEMAS CRÍTICOS E EM SISTEMAS DE INFORMAÇÃO – UM ESTUDO COMPARATIVO

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Professor Livre Docente, junto ao Departamento de Engenharia de Computação e Sistemas Digitais

Área de Concentração:
Confiabilidade e Segurança

São Paulo
2003

FICHA CATALOGRÁFICA

Almeida Jr., Jorge Rady de
Segurança em Sistemas Críticos e em Sistemas de Informação – Um Estudo Comparativo, São Paulo, 2003.
191p.

Tese (Livre Docência) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.
1. Sistemas Críticos quanto à Segurança. 2. Sistemas de Informação. 3. Sistemas Computacionais de Segurança. I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais.

À minha esposa Maria do Carmo, pelo carinho, compreensão e incentivo para que esta tese pudesse ser elaborada. Ao meu pai pelo apoio e constante presença na execução deste trabalho. À minha mãe, que embora não estivesse presente materialmente, iluminou, espiritualmente, minha mente.

AGRADECIMENTOS

A meus amigos e colegas do Grupo de Análise de Segurança, em especial aos Professores João Batista Camargo Junior, Selma Shin Shimizu Melnikoff e Paulo Sérgio Cugnasca pelo apoio e incentivo nesta empreitada.

Ao Professor Moacyr Martucci Junior pelo constante apoio à realização deste trabalho.

A todos os colegas do Departamento de Engenharia de Computação e Sistemas Digitais, que de alguma forma tenham contribuído para a concretização deste trabalho.

À minha esposa Maria do Carmo e ao meu Pai, pela compreensão, paciência e incentivo à elaboração deste trabalho. Agradeço pelas incontáveis horas em que não pude me dedicar a outras atividades, mas que foram recompensadas pela conclusão desta tese.

RESUMO

Neste trabalho é realizado um estudo comparativo entre os Sistemas Críticos quanto à Segurança e os Sistemas de Informação, bem como são estudadas as técnicas de garantia da segurança utilizadas nesses dois tipos de sistemas. Essas técnicas podem ser utilizadas de maneira isolada ou reunidas formando um único conjunto de técnicas para a garantia da segurança. Para que esse estudo comparativo seja completo, são apresentados os principais conceitos e aspectos referentes a Sistemas Críticos quanto à Segurança e a Sistemas de Informação, principalmente no que se refere à segurança dos mesmos. Também são definidos os significados de alguns termos utilizados em ambas as áreas de aplicação, buscando-se o esclarecimento de certas dúvidas comuns aos projetistas e usuários. Os resultados deste estudo apontam para uma aproximação gradual dos conceitos envolvidos nos Sistemas Críticos quanto à Segurança e dos Sistemas de Informação, na maioria de seus aspectos. Este trabalho revela-se de grande importância, considerando-se que os dois tipos de sistemas aqui estudados, ou seja, os Sistemas Críticos quanto à Segurança e os Sistemas de Informação constituem-se em elementos básicos do cotidiano das pessoas. Qualquer problema que possa afetar o funcionamento dos mesmos tem efeitos significativos na forma de condução das atividades de diversos setores econômicos e de produção.

ABSTRACT

In this work it is made a comparative study between Safety-Critical Systems and Information Systems, and it is analyzed the safety and security techniques used in both type of systems. These techniques can be used alone or joined, making one unique set of safety and security techniques. In order to make this comparative study as complete as possible, the main concepts referring to Safety-Critical Systems and Information Systems are presented, mainly in the safety and security aspects. There are also defined the meaning of some terms used in both application areas, explaining some doubts common to designers and users. The results of this study indicate to a gradual approach of the concepts about Safety-Critical Systems and Information Systems, in the most of its aspects. This work has great importance, considering that the Safety-Critical Systems and the Information Systems are basic elements of the people's quotidian. Any problem that can affect the functioning of these systems has significant effects in the conduction form of several economic and production sectors.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

ALARP – *As Low as Reasonably Possible*

ATC - *Air Traffic Control*

ATM - *Air Traffic Management*

B2B - *Business-to-Business*

B2C - *Business-to-Commerce*

BI – *Business Intelligence*

BSI – *British Standard Institute*

CC - *Common Criteria*

CENELEC - *Comité Europeen de Normalisation Electrotechnique*

CIM – *Computer Integrated Manufacturing*

CKO - *Chief Knowledge Officer*

CMM - *Capability Maturity Model*)

CNS CNS/ATM - *Communication, Navigation and Surveillance - Communication, Navigation and Surveillance*

CORBA – *Commom Object Request Broker*

COTS - *Commercial Off-The-Shelf*

CRM – *Customer Relationship Management*

DSO - *Departamental Security Officer*

DSS - *Decision Support Systems*

ERP – *Enterprise Resource Planning*

ETL – *Extraction, Transformation Load*

EUROCAE - *European Organization for Civil Aviation Electronics*

FAA - *Federal Aviation Administration*

FDA – *Food and Drug Administration*

GAS – Grupo de Análise de Segurança

HSE - *Health and Safety Executive*

HAZOP - *HAZard and Operability Analysis*

HTML – *Hyper Text Markup Language*

IAEA – *International Atomic Energy Agency*

IEC – *International Electrotechnical Commisions*

ISO - *International Standards Organization*

ITSEC – Information Technology *Security Evaluation Criteria*

JSTOR - *Journal Storage*

MRP – *Material Resource Planning*

MRPII – *Manufacturing Resource Planning*

MTBF - *Mean Time Between Failures*

MTTR - *Mean Time To Repair*

MTTUF - *Mean Time To Unsafe Failure*

NASA – *National Aeronautics and Space Administration*

NIST - *National Institute of Standards and Technology*

NMR - *N-Modular Redundancy*

NSA - *National Security Agency*

OLAP - *OnLine Analytical Process*

OMG – *Object Management Group*

ORB – *Object Request Broker*

RAID – *Redundant Array of Inexpensive Disks*

RAMS - *Reliability, Availability, Maintainability, Safety*

RTCA - *Requirements and Technical Concepts for Aviation*

SCM – *Supply Chain Management*

SGBD - Sistema Gerenciador de Bases de Dados

SEISP - *System Electronic Information Security Policy*

SIL - *Safey Integrity Level*

SIMS – *School of Information Management and Systems*

SSP - *System Security Policy*

SPI - *Software Process Improvement*

SPICE - S*oftware Process Improvement and Capability determination*

SPIRE - *Software Process Improvement in Regions of Europe*

TCSEC - *Trusted Computer System Evaluation Criteria*

TMR - *Triple Modular Redundancy*

VDM – *Viena Development Method*

WVTDB - *Web Based Video Text Data Base System*

1. INTRODUÇÃO

Este trabalho visa, inicialmente, apresentar os principais conceitos envolvidos na segurança de sistemas computacionais utilizados para o controle de Aplicações Críticas quanto à Segurança e de Sistemas de Informação. A partir da descrição desses conceitos, realiza-se um estudo comparativo desses aspectos, destacando-se pontos semelhantes e distintos, permitindo que se tirem conclusões se esses dois tipos de aplicações podem, de alguma forma, terem seus conceitos reunidos, formando uma única classe de sistemas.

1.1. Motivação

O ser humano sempre esteve sujeito a riscos. Antigamente esses riscos eram apenas naturais, tais como terremotos, vulcões e tempestades. Com o desenvolvimento da tecnologia diversos sistemas foram criados pelo homem, fazendo com que surgisse uma nova categoria de riscos, ou seja, os artificiais. Essa própria tecnologia vem colaborando para a diminuição dos riscos naturais, por exemplo, ajudando na previsão de fenômenos naturais, permitindo até o controle de alguns de seus efeitos.

As novas tecnologias trouxeram grandes benefícios à humanidade, permitindo a realização de atividades até então impensáveis com as antigas tecnologias. No entanto, praticamente qualquer sistema tem a si associados os riscos inerentes, sendo que o risco representado por um sistema pode ou não ser aceito pela sociedade, que em última análise, é quem define o conceito de risco aceitável. Isto significa que se faz necessária a realização de um balanço entre o benefício trazido pela nova tecnologia e o grau de risco a que a sociedade se dispõe a correr por aquele benefício. Essa avaliação depende de fatores sociais e culturais, como por exemplo, o valor que se atribui à propriedade, ao meio ambiente e à própria vida.

O desenvolvimento de novos Sistemas de Supervisão e Controle visa, além de monitorar e comandar os processos a que se destinam, reduzir o risco inerente de uma aplicação a um nível considerado aceitável. O risco pode ser visto como tendo relação direta com a freqüência de possíveis eventos perigosos e com a severidade de

suas conseqüências. Quanto maior a freqüência de um evento perigoso, maior o risco e quanto maior a severidade de suas conseqüências, maior o risco assumido.

O tipo de risco a que alguém pode estar exposto depende também do tipo de aplicação com que se possa estar trabalhando.

A primeira categoria de aplicações abordada neste trabalho são as Aplicações Críticas quanto à Segurança, nas quais o risco está diretamente ligado à segurança de pessoas, de propriedades e do meio ambiente. Ou seja, em caso de qualquer problema que possa vir a ocorrer com a aplicação, pode ser colocada em risco a integridade de seres humanos, a manutenção em perfeito estado do sistema em si e de toda estrutura agregada, tal como máquinas e edifícios e ainda a manutenção das condições do ambiente que envolva o sistema, como por exemplo, a atmosfera.

Como exemplo de Aplicações Críticas quanto à Segurança podem ser citadas usinas nucleares, plantas químicas e petroquímicas, aviação, sistemas ferroviários e metro-ferroviários e equipamentos médicos utilizados para tratamento de pacientes.

Por esses exemplos fica evidenciada a grande importância que tais aplicações representam para o homem, nos dias atuais. Todas são aplicações que não podem ter seu funcionamento prejudicado ou paralisado, não apenas pelo problema de acidentes, mas pelos benefícios que proporcionam à coletividade.

Cada vez mais o principal componente dos Sistemas de Supervisão e Controle de Aplicações Críticas quanto à Segurança é composto por computadores, cuja utilização é, e deverá continuar sendo, crescente no controle desses sistemas, substituindo os sistemas de controle baseados em componentes eletrônicos convencionais e mesmo em componentes mecânicos. Pode-se dizer que as principais justificativas para essa crescente utilização são a grande flexibilidade atingida pelos processadores, sua maior velocidade de resposta e um desempenho superior.

A utilização de processadores em Sistemas de Supervisão e Controle para Aplicações Críticas quanto à Segurança trouxe um novo conceito no que se refere ao risco aceito nesse tipo de aplicação. De fato, os dispositivos eletrônicos são de complexidade muito maior do que os dispositivos analógicos ou mesmo digitais de uma ou duas

décadas atrás. Aliada à complexidade dos componentes de hardware, vem acoplada a não menos complexa tarefa de produção de software.

São esses mesmos computadores que compõem o núcleo da segunda categoria de aplicações abordada neste trabalho, que são os Sistemas de Informação. Tendo em vista o ambiente de negócios extremamente competitivo dos dias atuais, não se concebe a existência de Sistemas de Informação sem a utilização intensiva de recursos computacionais.

A importância dos Sistemas de Informação reflete-se na relevância cada vez maior que a informação vem desempenhando nas organizações. A informação deve e vem sendo tratada como um bem da maior importância, cuja obtenção e manutenção são extremamente necessárias. Portanto, esforços realizados para um gerenciamento eficiente da informação e dos correspondentes Sistemas de Informação são plenamente justificados. É através da informação que as modernas organizações capacitam-se a atuar no ambiente, cada vez mais competitivo, representado pelo panorama atual da economia e da tecnologia.

A disponibilidade dos Sistemas de Informação normalmente deve ser integral, o que significa que o funcionamento deve ocorrer 24 horas por dia, nos 7 dias da semana. Portanto, um problema em um Sistema de Informação, considerando-se também os esquemas de contingência, normalmente significa um prejuízo muito grande para as atividades de uma organização.

Aliado ao fator da disponibilidade, outros fatores também devem ser levados em conta, tais como a garantia de um desempenho compatível com as especificações, a segurança dos dados armazenados contra invasões ou furto de informação, a manutenção permanente da consistência dos dados e a facilidade de utilização.

Nos Sistemas de Informação, o risco toma outra forma. Nesse caso, o risco que se corre não está diretamente ligado a situações de calamidade ou de acidentes, mas sim com a perda ou a adulteração de dados, ou ainda com a invasão do sistema por pessoas ou sistemas não autorizados.

Como exemplo de Sistemas de Informação podem ser citados os sistemas de automação bancária, sistemas de apoio à decisão, sistemas de apoio à produção, sistema de gerenciamento de relações com os clientes e Intranets, dentre outros.

Pode-se até afirmar que alguns Sistemas de Informação estão se tornando críticos. Nessa linha de raciocínio, um sistema pode ser dito crítico quando a sua falha leva o sistema a apresentar conseqüências inaceitáveis. Alguns exemplos podem ser citados, tais como uma falha em um sistema de crédito pode levar a grandes perdas financeiras, uma falha em uma central de atendimento pode tornar indisponível o atendimento a clientes atuais e a possíveis novos clientes, e assim por diante.

Devido a esse complexo panorama apresentado, faz-se necessário um estudo detalhado de Aplicações Críticas quanto à Segurança e de Sistemas de Informação, de forma a permitir uma comparação criteriosa de seus principais aspectos.

1.2. Nomenclatura Utilizada

É importante que se estabeleça uma nomenclatura mais adequada às até aqui denominadas Aplicações Críticas quanto à Segurança. Na literatura há, de uma forma geral, a utilização do termo sistema para denominar tanto o Sistema de Supervisão e Controle, responsável pela recepção dos sinais de entrada, seu processamento e a respectiva geração dos sinais de saída, quanto para denominar a Aplicação Crítica quanto à Segurança, supervisionada e controlada por esse sistema.

Por exemplo, utiliza-se o termo sistema tanto para denominar uma usina nuclear responsável pela geração de energia, quanto para seu Sistema de Supervisão e Controle. No entanto, esta forma de denominação causa uma certa ambigüidade, pois se está fazendo utilização indevida da palavra sistema para designar uma aplicação.

Desta forma, adotou-se, neste trabalho, o termo Aplicação Crítica quanto à Segurança, ou mais resumidamente, Aplicação Crítica, para denominar o objeto supervisionado e controlado e o termo Sistema de Supervisão e Controle, ou mais sucintamente Sistema Crítico, para designar os equipamentos, circuitos e seu

software associado, os quais realizam a supervisão e controle sobre a Aplicação Crítica.

A figura 1.1 ilustra esses conceitos. Por exemplo, a Aplicação Crítica poderia ser representada por uma planta química ou por um avião e o Sistema Crítico pelos circuitos e por seu software, específicos a cada aplicação.

Figura 1.1 - Aplicações Críticas quanto à Segurança e sua Supervisão e Controle

A razão para essa simplificação é não tornar o texto muito denso quando se fizerem necessárias referências a aplicações com requisitos de segurança e seus Sistemas de Supervisão e Controle.

O mesmo problema não ocorre com relação aos Sistemas de Informação, cuja denominação não necessita de simplificação.

Há outro termo que deve ter sua denominação padronizada. No caso de Sistemas Críticos, as medidas de segurança assumem um caráter diferenciado das medidas de segurança que um Sistema de Informação deve receber. Embora haja essa diferenciação de competências, na língua portuguesa essas duas atividades recebem a mesma denominação, ou seja, segurança, enquanto que na língua inglesa há dois termos distintos. O termo *safety* é utilizado para se fazer referência à segurança dos Sistemas Críticos, enquanto que o termo *security* é utilizado para referenciar a segurança dos Sistemas de Informação. De forma a estabelecer uma distinção entre esses dois conceitos, neste trabalho é adotada a denominação Segurança Crítica para a segurança dos Sistemas Críticos e Segurança de Informação para a segurança dos Sistemas de Informação.

1.3. Objetivos

O objetivo central deste trabalho é o de realizar um estudo comparativo entre os Sistemas Críticos e os Sistemas de Informação, bem como das técnicas de garantia da segurança utilizadas nesses dois tipos de sistemas. Essas técnicas poderiam ser utilizadas de maneira isolada ou reunidas, formando um único conjunto de técnicas para a garantia da segurança.

Um segundo objetivo é o de reunir e apresentar os principais conceitos e aspectos referentes a esses dois tipos de sistemas, ou seja, Sistemas Críticos e Sistemas de Informação, principalmente no que se refere à segurança dos mesmos.

Outro objetivo que se coloca é o de se definir de maneira precisa o significado de alguns termos utilizados em ambas as áreas, buscando-se o esclarecimento de certas dúvidas comuns aos projetistas e usuários das duas áreas de aplicação.

Conforme citado no item anterior, modernamente, tanto os Sistemas Críticos, quanto os Sistemas de Informação fazem uso intensivo de recursos computacionais, em alguns casos compartilhando as mesmas técnicas de desenvolvimento e projeto do hardware e software associados.

Os Sistemas Críticos e os Sistemas de Informação têm de ser protegidos, cada um contra seus tipos específicos de problemas associados. Em ambas categorias de sistemas devem ser adotadas medidas para manter o seu perfeito funcionamento e segurança, impedindo a ocorrência de situações ou estados perigosos nos sistemas.

As características das técnicas de proteção, visando a garantia da segurança de Sistemas Críticos e de Sistemas de Informação apresentam uma série de aspectos semelhantes, mas também diversos pontos distintos.

Nos Sistemas Críticos, as técnicas de proteção buscam, basicamente, evitar a ocorrência de estados inseguros, ou se isso não for possível, levar os sistemas a um estado sabidamente seguro, no caso de ocorrência de alguma falha. Dentre as principais técnicas utilizadas pode-se citar a utilização de módulos redundantes no controle dos sistemas, aliada ao emprego de circuitos comparadores ou votadores das saídas dos módulos redundantes. No desenvolvimento do software busca-se a

utilização intensiva de diagnósticos e de programação defensiva, sempre visando a eliminação de erros e a produção de um software mais robusto.

Nos Sistemas de Informação são utilizadas técnicas de identificação e autenticação, técnicas de segurança na comunicação através de protocolos, criptografia, *firewalls*, dentre outros.

Dentre as técnicas de proteção comuns aos Sistemas Críticos e aos Sistemas de Informação, pode-se citar a utilização de módulos redundantes e o uso de codificação das informações.

Destacando novamente, a questão que se coloca neste trabalho é porque não fazer uma utilização conjunta das técnicas e requisitos utilizados em Sistemas Críticos e em Sistemas de Informação, considerando-se que, no que se refere às questões de segurança, há muitas características comuns aos dois tipos de aplicação.

Uma visão conjunta de Sistemas Críticos e de Sistemas de Informação pode permitir um investimento mais eficiente de recursos humanos, técnicos e econômicos em diversos aspectos, tais como projeto, definição de requisitos de segurança, implementação dos sistemas e análise de segurança. Pode-se até pensar que, utilizando-se as melhores técnicas de cada área, os sistemas resultantes poderão apresentar melhores características, não apenas no aspecto segurança, mas também na disponibilidade e no desempenho.

Portanto, os objetivos colocados no início desta seção revelam-se de grande importância, considerando-se que os dois tipos de sistemas aqui estudados, ou seja, os Sistemas Críticos e os Sistemas de Informação constituem-se em elementos básicos do cotidiano das pessoas. Qualquer problema que possa afetar o funcionamento dos mesmos tem efeitos significativos na forma de condução das atividades de diversos setores econômicos e de produção.

1.4. Organização do Trabalho

O capítulo 2 descreve as principais características de sistemas diretamente ligados à segurança, ou seja, os Sistemas Críticos. São descritos os principais conceitos envolvidos nesse tipo de sistemas, a importância da existência de uma cultura de segurança nas organizações e o aspecto vital de se desenvolver requisitos diretamente relacionados à segurança.

Também são apresentados os conceitos ligados à arquitetura desses sistemas, tanto no que se refere ao software, quanto ao hardware. Detalha-se uma metodologia de análise de segurança voltada a Sistemas Críticos. Por fim, apresentam-se algumas das principais Aplicações Críticas atualmente existentes.

O foco principal do capítulo 3 reside nos Sistemas de Informação, destacando-se inicialmente os principais conceitos desse tipo de sistemas. A cultura de Segurança de Informação e os Requisitos de Segurança aplicados a Sistemas de Informação, fatores de grande valia, também são detalhados nesse capítulo. Em seguida, são descritas as tecnologias utilizadas para sua implementação, bem como os principais tipos de aplicação desses sistemas. Destacam-se também as técnicas de armazenamento e recuperação de dados, extremamente importantes nos Sistemas de Informação.

No capítulo 4 é feita uma comparação dos dois conceitos de segurança, que são a Segurança Crítica e a Segurança de Informação, destacando-se suas principais semelhanças e distinções, propondo-se uma integração parcial de seus conceitos. Essa integração pode ser atingida, em um primeiro momento, através da aplicação isolada das técnicas já existentes em cada uma das áreas, e em um segundo momento através da adaptação dessas mesmas técnicas, visando sua aplicação às duas áreas, ou seja, os Sistemas de Informação os Sistemas Críticos.

Nesse mesmo capítulo são comparados, um a um, os aspectos descritos nos capítulos 2 e 3, de forma a se obter subsídios para o desenvolvimento de uma conclusão fundamentada sobre as características básicas dos sistemas e como os dois conceitos

de segurança podem ser reunidos e mesclados de forma a produzir um resultado mais robusto.

No capítulo 5 são descritos os trabalhos desenvolvidos e em desenvolvimento referentes a essas duas linhas de pesquisa, ou seja, os Sistemas Críticos e os Sistemas de Informação. Essas atividades vêm sendo conduzidas através de orientações de alunos de mestrado e doutorado, bem como pela participação em projetos de pesquisa e extensão universitária. Nesse capítulo também são propostos novos temas a serem estudados e pesquisados, de forma a dar seqüência ao tema proposto nesta Tese de Livre Docência.

Finalmente no capítulo 6 são apresentadas as principais conclusões, ressaltando-se as principais contribuições deste trabalho.

2. SISTEMAS CRÍTICOS

Aplicações Críticas são aquelas nas quais uma falha possa ter como conseqüência acidentes que venham a provocar sérios danos materiais, danos ao ambiente, ou ainda representar perigo à vida humana, seja de operadores, seja da população possivelmente atingida por uma falha do Sistema Crítico dessas aplicações (WILLIAMSON, 1997). Desta forma, devem ser utilizadas técnicas que busquem prevenir a ocorrência de acidentes, sendo que quanto maiores ou mais graves forem as perdas ou prejuízos decorrentes de falhas do Sistema Crítico, mais se justificam esforços e recursos investidos na prevenção desses acidentes (SAEED et al., 1991).

As atividades relativas à Segurança Crítica devem ser iniciadas já na concepção do Sistema Crítico e devem ter seqüência ao longo de seu projeto, produção, teste, operação e manutenção. O projeto deve enfatizar, desde o seu início, os aspectos relativos à Segurança Crítica, considerando-se tal prática mais eficaz, pois a inclusão de componentes a posteriori não tem demonstrado bons resultados, nem do ponto de vista técnico, nem do ponto de vista de custos do sistema. A Segurança Crítica deve ser vista como um todo, ou seja, não é suficiente garanti-la apenas em partes ou subsistemas de um sistema maior.

Os problemas no funcionamento de um Sistema Crítico podem advir de falhas no próprio sistema, de entradas impróprias não previstas ou não cobertas pelos mecanismos de detecção, ou ainda por procedimentos operacionais incorretos. São esses problemas que podem provocar a ocorrência de situações perigosas, podendo ou não resultar em acidentes (ALMEIDA; CAMARGO, 1996).

Tendo em vista que a quantidade e variedade de Sistemas Críticos têm apresentado grande crescimento, podendo ocasionar cada vez problemas mais graves, torna-se necessária a realização de atividades que visem obter uma prevenção do número de situações perigosas, de acidentes, ou ainda uma diminuição de suas conseqüências. O desenvolvimento desses sistemas é, normalmente, controlado por órgãos reguladores, que estabelecem critérios de certificação de sistemas em cada área particular.

É o caso das normas IEC 61508 (IEC, 1997) e ENV 50129 (CENELEC, 1998a), que determinam uma relação entre as atividades ligadas à garantia da Segurança Crítica e o Nível de Integridade de Segurança - SIL (*Safey Integrity Level*) do sistema. Este termo designa os Níveis de Integridade exigidos para a implementação de Sistemas Críticos. O Nível de Integridade atribuído a um sistema determina quais exigências devem ser adotadas, em termos de requisitos, projeto, implementação e análise. Quanto maior o Nível de Integridade exigido para uma aplicação, maiores os cuidados a serem tomados na implantação de um sistema.

A norma ENV 50129 (CENELEC, 1998a) define quatro Níveis de Integridade de Segurança, numerando-os de 1 a 4, sendo 4 o nível mais alto de segurança. As denominações atribuídas pela norma a cada Nível de Integridade de Segurança são: nível 4 – muito alto, nível 3 – alto, nível 2 – médio e nível 1 – baixo. A norma IEC 61508 (IEC, 1997) também define quatro Níveis de Integridade de Segurança, numerando-os também de 1 a 4, sem, no entanto, nomeá-los.

Ambas as normas apresentam tabelas de valores máximos permitidos para as taxas de falhas, em cada um dos quatro Níveis de Integridade de Segurança. A norma ENV 50129 (CENELEC, 1998a) estabelece padrões mais rígidos para todos os Níveis de Integridade, através da exigência de menores taxas de falhas. Isto se deve ao fato de que esta norma é voltada a um tipo específico de Aplicação Crítica, que são os sistemas ferroviários, enquanto que a norma IEC 61508 é voltada a sistemas industriais em geral, cujo nível médio de exigência é menor.

Outras normas também especificam Níveis de Integridade de Segurança, efetuando a classificação dos Sistemas Críticos em quatro ou mais níveis.

2.1. Segurança de Sistemas Críticos

Antigos Sistemas Críticos vêm sendo substituídos cada vez mais freqüentemente por sistemas computadorizados. Algumas das vantagens decorrentes dessa substituição são a maior capacidade de controle, a velocidade de resposta e o desempenho, amplamente superiores às técnicas até então utilizadas, principalmente representadas por circuitos eletrônicos convencionais e sistemas eletromecânicos. Além disso, torna-se possível a inclusão de novas funções, até então não disponíveis com as antigas tecnologias.

Por outro lado, com a utilização intensiva de Sistemas Críticos computadorizados, surge o problema da certificação desses Sistemas, tendo em vista a grande complexidade das novas formas de implementação. Portanto, a certificação dos antigos sistemas de supervisão e controle também teve de sofrer um processo de atualização, de forma a acompanhar as novas tarefas de verificação da correção de funcionamento, tanto do hardware, quanto do software.

É de fundamental importância o estabelecimento de uma metodologia de Análise de Segurança Crítica, visando a verificação de todos os aspectos envolvidos no funcionamento de um Sistema Crítico, sejam eles relativos ao hardware, ao software ou à operação (ALMEIDA et al., 2002a).

Diversos tipos de indústrias, tais como plantas químicas e siderúrgicas, indústria da aviação, plantas nucleares, indústria automobilística, etc., vêm fazendo uso intensivo de Sistemas Críticos computadorizados. Estes exemplos demonstram a grande importância de uma busca constante por novas e melhores técnicas que visem a garantia da Segurança Crítica.

A garantia da Segurança Crítica é essencial para que sua operação possa ser feita dentro de níveis de riscos aceitáveis. Para que a Segurança Crítica seja mantida dentro de padrões adequados, devem ser utilizadas técnicas que permitam prevenir os acidentes ou, em última instância, minimizar suas conseqüências.

2.1.1. Conceitos Básicos de Segurança Crítica

A Segurança Crítica é definida como a probabilidade, em um período de tempo, de que um sistema não atinja um estado considerado inseguro ou perigoso, ou seja, não fique exposto a um acidente. Um estado inseguro é definido como sendo parte de um subconjunto dos estados de falha de um sistema.

Mais formalmente, Segurança Crítica é a probabilidade de um sistema, em um determinado período de tempo Δt, desempenhar corretamente suas funções, ou falhar sem comprometer a integridade de pessoas e do meio ambiente, dado que este sistema estava seguro no instante inicial.

Três outros conceitos importantes guardam relação direta com a Segurança Crítica, que são a confiabilidade, a disponibilidade e a mantenabilidade. Por relação direta, entende-se que, quanto maior a confiabilidade e a disponibilidade e quanto mais fácil for a manutenção do Sistema Crítico, maior a probabilidade de que a Segurança Crítica atinja melhores níveis, principalmente no que se refere a menores probabilidades de atingir estados inseguros.

A confiabilidade indica a probabilidade de um sistema permanecer sem falhas por um período de tempo, considerando que, no instante inicial, o mesmo se encontrava funcionando corretamente. A disponibilidade é a medida da probabilidade de um sistema estar sem falha em um determinado instante de tempo. Por mantenabilidade entende-se a habilidade de um sistema ser mantido e, em termos quantitativos, é representada pelo valor do MTTR (*Mean Time To Repair*). Já a manutenção representa a ação tomada para manter um sistema em seu estado operacional ou para fazer com que retorne a esse estado.

Há diversas características de desempenho, operação e manutenção que podem ser conflitantes com aspectos de Segurança Crítica. A decisão entre qual deve ser a característica predominante ou de como os conflitos devem ser resolvidos depende de compromissos de projeto a serem assumidos.

Outra definição importante é a da integridade, que abrange dois níveis, que são a integridade da funcionalidade e a integridade de dados. A integridade da

funcionalidade do Sistema Crítico representa a habilidade do sistema em detectar falhas em sua operação e informá-las aos operadores. Por outro lado, a integridade de dados representa a habilidade de um sistema em prevenir danos a seus dados, através de sua detecção e possível correção de erros.

Um conceito diretamente ligado com a Segurança Crítica é a verificação da aderência do funcionamento do Sistema Crítico com respeito a suas especificações. Por esta razão, a especificação deve ser completa, consistente e compreensível, não devendo conter ambigüidades. Quando o comportamento de um sistema se desvia daquele especificado, tem-se a ocorrência de um mau funcionamento ou disfunção, que se refere ao comportamento externo inadequado do sistema, comportamento esse resultante de problemas internos. Tais problemas internos são chamados de erros e são, por sua vez, causados por componentes ou módulos com falhas. A falha de um componente ou módulo é causada por problemas mecânicos ou elétricos, considerado-se o hardware, ou por problemas no software. A figura 2.1 representa o encadeamento entre estes três conceitos.

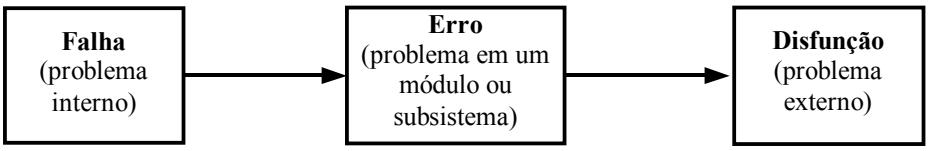

Figura 2.1 - Interconexão entre os Conceitos de Falha, Erro e Disfunção

É importante notar que nem todas as falhas resultam em erros e, da mesma forma, nem todos os erros produzem disfunções. Uma falha pode ficar contida, não levando problemas a módulos ou subsistemas, não provocando erros. De maneira similar, um erro pode permanecer restrito ao módulo ou subsistema, não sendo exteriorizado na forma de uma disfunção.

No que se refere aos tipos de falhas, podem ser identificados três tipos, que são as falhas transientes, as falhas intermitentes e as falhas permanentes. As falhas do tipo transiente não são diretamente inerentes ao hardware ou ao software do Sistema Crítico, sendo normalmente ocasionadas por fenômenos externos, perdurando apenas durante a existência de tais fenômenos. Interferências eletromagnéticas constituem um exemplo de uma falha transiente. As falhas do tipo intermitente são inerentes ao hardware do Sistema Crítico, manifestando-se de acordo com a ocorrência de

determinadas condições pré-estabelecidas no circuito. Como exemplo de falha intermitente pode-se citar um componente que apresente problemas apenas quando aquecido. Finalmente, falhas do tipo permanente manifestam-se de forma contínua no sistema, até que o reparo seja feito. Falhas deste tipo podem ser de hardware ou de software.

Além desses três tipos, os modos de falhas dividem-se em dois domínios, que são a falha de valor e a falha de tempo. No caso de falha de valor, valores associados a tarefas apresentam-se incorretos. No caso de falha de tempo, uma tarefa é concluída fora do intervalo de tempo permitido, ou seja, muito cedo ou muito tarde, ou então nem é concluída.

2.1.2. Prevenção e Tolerância a Falhas

Em Sistemas Críticos é sempre necessário que se tenha implementado algum tipo de mecanismo de tolerância a falhas, que se constitui na habilidade de um sistema ou componente continuar sua operação normal, mesmo com a presença de falhas de hardware ou de software. A tolerância a falhas pode visar uma melhor disponibilidade do sistema, uma maior segurança do mesmo ou a manutenção da integridade de seus dados. A implementação da tolerância a falhas não significa abandonar a técnica de prevenção de falhas, mas sim obter um maior resguardo contra falhas do sistema.

A prevenção de falhas constitui uma primeira barreira para que sejam evitadas disfunções no Sistema Crítico. Utilizam-se técnicas para a prevenção de falhas tanto a nível do hardware, quanto a nível do software. Para que seja possível a prevenção de falhas no hardware, pode-se utilizar componentes mais confiáveis, técnicas mais refinadas de projeto e de interconexão de componentes, além de uma documentação completa de desenvolvimento e de implementação, colaborando com a tarefa de manutenção. No tocante ao software, as técnicas utilizadas para a prevenção de falhas concentram-se na elaboração de especificações rigorosas de requisitos e na utilização de metodologias adequadas de projeto, além de técnicas de verificação e validação. A documentação completa também faz parte do ciclo de desenvolvimento

de software, colaborando, como no hardware, não apenas em seu desenvolvimento, mas também na manutenção do sistema.

Outra forma de se incrementar a Segurança Crítica dos sistemas é mascarando falhas, o que é conseguido através da implementação de redundâncias no Sistema Crítico. O mascaramento significa que, mesmo na ocorrência de falhas, as mesmas não serão percebidas nas saídas do sistema, em virtude da inclusão de módulos redundantes. Por redundância entende-se a inclusão, no Sistema Crítico, de módulos complementares, que desempenham funções similares às já exercidas por outros módulos do sistema. Se for detectada a ocorrência de falhas, estas devem ser toleradas, ou seja, não devem causar efeitos negativos ao sistema. Isto é conseguido através da detecção da falha, sua localização, respectiva contenção de seus efeitos e finalmente a recuperação dessa falha (HATTON, 2001).

A eficiência dos métodos de recuperação depende da eficiência do fator de cobertura de falhas, que se constitui na medida da eficiência do sistema em detectar falhas que venham a ocorrer. Quanto melhor a eficiência nessa detecção, melhor o fator de cobertura, que pode ser aumentado por meio da utilização de diagnósticos, sejam implementados diretamente por meio de hardware, sejam implementados por meio de software (CAMARGO et al., 2001).

2.1.3. Riscos

Mesmo com todos os mecanismos descritos no item anterior, sempre há uma probabilidade, mesmo que baixa, da ocorrência de situações perigosas e até de acidentes em uma Aplicação Crítica. Essa probabilidade é definida pelo risco do Sistema Crítico apresentar algum tipo de disfunção.

A aceitabilidade de um determinado nível de risco é determinada pelos benefícios associados à Aplicação Crítica e, conseqüentemente, seus riscos, bem como pelos esforços necessários para que se consiga a redução desses riscos. Riscos com conseqüências catastróficas e que ocorram freqüentemente não são toleráveis em nenhuma hipótese. Por outro lado, riscos com conseqüências não significativas, mesmo com ocorrência freqüente, podem ser aceitáveis.

A norma IEC 61508 classifica o risco em três níveis (IEC, 1997):

- Risco Intolerável: as conseqüências do risco são intoleráveis e sua ocorrência não pode ser justificada;
- Risco Inaceitável: as conseqüências do risco são inaceitáveis, embora possam ser suportadas sob certas condições;
- Risco Negligenciável: as conseqüências do risco são insignificantes e podem ser desprezadas.

No caso de Sistemas Críticos, um determinado risco é aceitável se atingir um nível baixo o suficiente, de forma que reduções maiores não sejam justificáveis dos pontos de vista técnico e econômico. Esse é o princípio ALARP – *As Low as Reasonably Possible*, ou seja, o risco deve ser tão baixo quanto o razoavelmente praticável ou implementável (IEC, 1997). É importante considerar que um risco não é aceitável se ele puder ser facilmente reduzido. Portanto, mesmo um sistema com um nível de risco muito pequeno pode ser considerado como inaceitável se o seu nível de risco puder ser facilmente reduzido. Similarmente, um sistema que tenha um nível de risco significante pode satisfazer aos requisitos se ele oferecer benefícios suficientes e reduções do risco forem consideradas impraticáveis. A figura 2.2 representa o princípio ALARP.

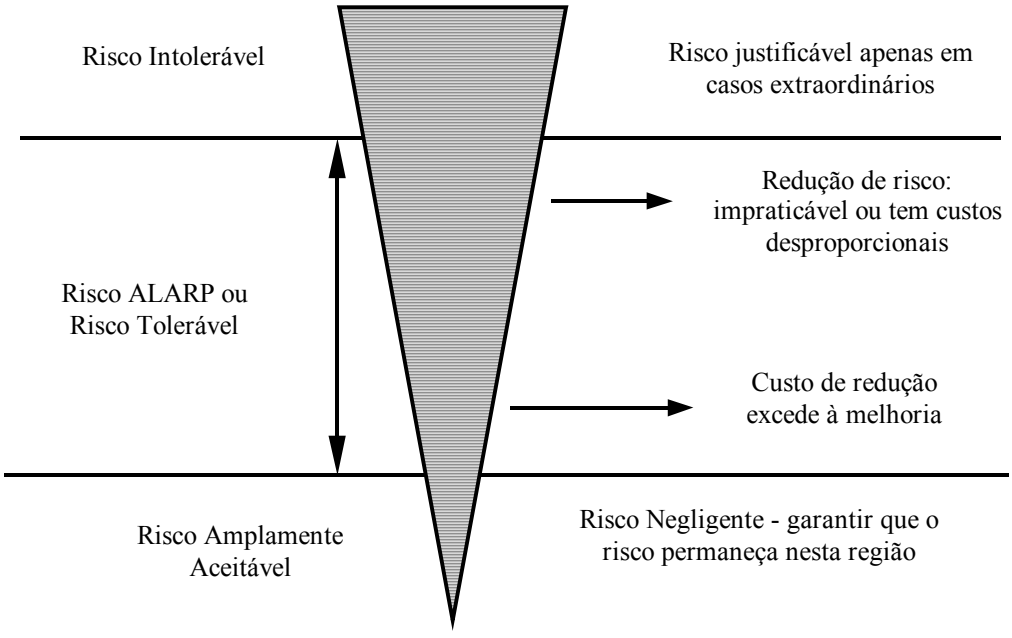

Figura 2.2 – Princípio ALARP – *As Low as Reasonably Possible*

Neste item foram apresentados os principais conceitos relacionados à Segurança Crítica. Dando continuidade à descrição dos aspectos mais relevantes da Segurança Crítica, no próximo item é discutida a importância em se ter estabelecida uma cultura de Segurança Crítica em instituições responsáveis pelo projeto, operação e análise desses sistemas.

2.2. Cultura de Segurança em Sistemas Críticos

A avaliação da Segurança Crítica de um Sistema Crítico deve estar inserida dentro de uma cultura global de Segurança Crítica das organizações, envolvendo a operadora da aplicação, fornecedores de sistemas e subsistemas e um órgão certificador. A segurança deve ser alvo do projeto em todas as fases do ciclo de vida do sistema, envolvendo também os aspectos de treinamento e motivação de profissionais envolvidos. A harmonia e conscientização do conceito de Segurança Crítica é que irão realmente garantir a ocorrência de um menor número de situações inseguras para a Aplicação Crítica.

Podem ocorrer conflitos entre as características especificadas para um Sistema Crítico, como por exemplo, uma especificação que abranja a cobertura de todas as situações potencialmente perigosas conhecidas, aliada a restrições de custo e de prazo de desenvolvimento. É necessário estabelecer compromissos para o desenvolvimento do projeto, de forma a contemplar satisfatoriamente a todos os requisitos especificados.

Deve ser utilizada, normalmente, uma combinação de diversas técnicas e procedimentos para que sejam atingidos os níveis desejados para a Segurança Crítica, tendo em vista que, raramente, a aplicação de apenas uma técnica irá fazer com que sejam garantidos os padrões de segurança exigidos. Mais uma vez deve-se frisar que todo o esforço em se garantir a Segurança Crítica deve estar inserido em um plano global de Segurança Crítica de toda a organização.

Dentro desse plano global de Segurança Crítica, sempre deve estar inserido um programa de treinamento do corpo técnico. Um dos objetivos desse treinamento deve

ser o de manter o espírito de colaboração e de atenção a todo e qualquer evento que possa representar ameaça à Segurança Crítica.

A preocupação com a Segurança Crítica deve ser constante, e não deve representar assunto secreto ou confidencial dentro da organização. Pelo contrário, as normas que regem a garantia da Segurança Crítica devem ser amplamente divulgadas, preparando a todos para o combate a eventuais problemas que possam vir a ocorrer em decorrência de falhas no Sistema Crítico.

Mesmo que parte ou toda a operação de um Sistema Crítico seja automatizada, deve haver uma equipe capacitada a assumir a operação do sistema, mesmo que de forma parcial, em caso de pane nos equipamentos.

Operadores habituados com o funcionamento de um Sistema Crítico podem vir a acreditar que um acidente não possa vir a ocorrer, pois não seria possível que houvesse a ocorrência, simultaneamente, de um número muito grande de condições adversas, o que, normalmente, não é verdade. Este tipo de comportamento indica que pode estar ocorrendo complacência e autoconfiança excessivas com relação ao Sistema Crítico (LEVESON, 1995).

Ainda com relação à complacência, outro fator importante é o caso em que um sistema opera por longos períodos de tempo sem falhas. Acredita-se que o sistema não possa mais falhar, o que se constitui em uma suposição incorreta.

As condições perigosas mais evidentes são as que recebem maior atenção e são, conseqüentemente, controladas, enquanto que aquelas condições com menor probabilidade de ocorrência acabam por ser desprezadas. É comum se verificar que, após um acidente, sua causa se constituía em um evento conhecido, que foi desprezado, considerando sua ocorrência como altamente improvável.

Também não podem ser ignorados sinais de alarme, pois os acidentes são, freqüentemente, precedidos por alertas, ou por uma série de ocorrências menores, geralmente ignoradas, pois não se acredita que algo mais grave ainda possa vir a acontecer.

Outro fator de grande importância é a realimentação que deve existir a respeito de acidentes ocorridos em outros sistemas similares ao sistema em questão, pois essas informações podem e devem ser efetivamente utilizadas na prevenção de novos acidentes.

As deficiências na cultura de Segurança Crítica de uma organização podem refletir-se em todos seus membros, desde a alta direção, chegando até os técnicos responsáveis pelo funcionamento da aplicação.

Tendo isto em vista, outro fator de impacto na causa de acidentes refere-se à baixa prioridade dada à Segurança Crítica por parte da alta administração das organizações, a qual deve fornecer o suporte indispensável a tais atividades. Agências governamentais e grupos de usuários têm, como objetivo, aumentar essa prioridade, buscando melhores condições para incremento da Segurança Crítica.

Em resumo, não deve haver relaxamento no que se refere à garantia das condições seguras, sendo que todos em uma organização, desde a equipe técnica até sua alta direção, devem sempre estar atentos a todos eventos que, de alguma forma, possam por em risco a Segurança Crítica de uma Aplicação.

Conforme destacado no decorrer deste item, pode-se perceber a grande importância que a especificação de requisitos de segurança desempenha em Sistemas Críticos. Esses requisitos são descritos no próximo item.

2.3. Requisitos de Segurança Aplicáveis a Sistemas Críticos

Cada um dos objetivos de um Sistema Crítico deve ser avaliado, considerando-se o conjunto de todos os requisitos, ou seja, devem ser ponderados todos os aspectos vitais à aplicação.

Os requisitos de Sistemas Críticos podem ser encarados como possuindo três princípios básicos, que são o de evitar a ocorrência de condições consideradas como perigosas, prevenir que, mesmo na ocorrência de condições perigosas, ocorram acidentes e proteger contra efeitos de possíveis acidentes que venham a ocorrer.

Desta forma, o objetivo de uma especificação de requisitos para Sistemas Críticos é restringir a ocorrência de condições ou estados perigosos, buscando a redução do número desses estados através da definição de requisitos globais de Segurança Crítica.

Em alguns casos, é comum que se gere um documento específico, contendo os Requisitos de Segurança Crítica do sistema. Tal documento deve detalhar as funções que o sistema deve executar, bem como algumas ações que o sistema não deve realizar, de forma a que se atinja a o grau de Segurança Crítica desejado.

Os Requisitos de Segurança Crítica são específicos a cada Aplicação Crítica, mas há diversos aspectos comuns, como por exemplo: a identificação de condições perigosas associadas ao sistema, a classificação dessas condições e a determinação de métodos para tratamento das mesmas.

Os principais requisitos que se colocam com relação a Sistemas Críticos são aqueles não diretamente ligados às funcionalidades do sistema. Sendo assim, os requisitos mais importantes no contexto da Segurança Crítica são a confiabilidade, o desempenho, a usabilidade e a própria Segurança Crítica (STOREY, 1996).

Podem ocorrer situações conflitantes entre os requisitos estabelecidos para um sistema, como por exemplo, o desempenho de um sistema pode ser prejudicado pela adição de código redundante em sua programação, código esse que vise a detecção de erros, tendo como objetivo aumentar a confiabilidade do sistema.

Situação semelhante ocorre no caso de se efetuar a validação do agente emissor de um comando, verificando se o mesmo tem autorização para tal operação. Esse tipo de verificação pode envolver operações adicionais na utilização do sistema, prejudicando sua usabilidade.

Outro exemplo que pode ser citado é, se em decorrência de falhas, puder ser atingido um estado inseguro, mesmo que remotamente. Tal fato pode provocar o acionamento freqüente de mecanismos de proteção, que, por exemplo, desliguem o sistema, tornando-o indisponível. Neste caso se estará favorecendo a Segurança Crítica em detrimento da disponibilidade do sistema.

Outro grupo de requisitos a ser especificado consiste em valores numéricos para as taxas de falhas dos módulos que compõem o hardware de um Sistema Crítico. Devem ser especificadas tanto as taxas médias de falhas, quanto os tempos médios exigidos para o reparo dos sistemas.

Segundo Kotonya e Sommerville (1998), as principais características do conjunto básico de requisitos de Sistemas Críticos são:

a) Requisitos de Confiabilidade

São os requisitos diretamente ligados à disponibilidade e à taxa de falhas (quão freqüentemente o sistema deixa de desempenhar sua função). Ambos, disponibilidade e taxa de falhas, são expressos de forma quantitativa.

b) Requisitos de Desempenho

Os tipos de requisitos de desempenho especificados são os tempos de resposta aceitáveis por usuários e por outros sistemas que possuam interfaces com o sistema sob estudo, a quantidade de dados processados em um determinado período de tempo e os períodos determinados para a obtenção de sinais de entrada e para a geração de sinais de saída. Estes parâmetros são do tipo quantitativo,

c) Requisitos de Segurança Crítica

Nesta categoria de requisitos, os objetivos são assegurar uma operação sem a ocorrência de situações consideradas perigosas e determinar a adequação de sistemas de proteção. Informalmente, pode-se dizer que são requisitos que estabelecem o que o sistema não pode fazer, restringindo a liberdade do projetista. São ainda determinadas todas as condições inaceitáveis ou indesejáveis para o sistema. Os requisitos de segurança crítica são considerados do tipo qualitativo.

d) Requisitos de Segurança de Informação

Tais requisitos têm como objetivo garantir que não seja feito o acesso ao sistema e a seus dados, por pessoas ou sistemas não autorizados. Exemplos de requisitos deste tipo são, manter permissões de acesso sob controle do administrador do sistema, efetuar cópias de segurança a determinados períodos e armazená-las em local seguro

ou ainda efetuar a criptografia em todas comunicações externas realizadas. A Segurança de Informação é vital para a manutenção da Segurança Crítica.

e) Requisitos de Usabilidade

Referem-se à interface do usuário e suas interações com o sistema. Exemplos de requisitos deste tipo são o tempo de aprendizado de uso do sistema e a gravidade ou importância de erros na operação.

Vale a pena ressaltar que Kotonya e Sommerville (1998) destacam a Segurança de Informação como um fator importante em Sistemas Críticos.

Após terem sido descritos os principais aspectos relativos à aplicação de Requisitos de Segurança a Sistemas Críticos, devem merecer atenção as características exibidas pelos principais tipos de implementações de Sistemas Críticos, o que é feito no item a seguir.

2.4. Implementação de Sistemas Críticos

Praticamente todos os novos Sistemas Críticos vêm se utilizando da tecnologia de processadores para sua implementação. As principais causas para as falhas desses sistemas provêm de erros na especificação de requisitos do Sistema Crítico, falhas em componentes do hardware e falhas de projeto, sejam essas falhas advindas do projeto do hardware ou do projeto do software.

O hardware utilizado no controle e supervisão de Aplicações Críticas apresenta complexidade cada vez maior, fazendo com que a previsibilidade de seus modos de falha seja cada vez mais dificultada. Os modos de falhas do hardware que compõe um computador são extremamente complexos e difíceis de se prever. No que se refere ao software, embora este represente um fator de extrema flexibilidade, representa também um dos principais problemas na utilização de computadores em Aplicações Críticas.

O principal motivo para tal afirmação está na verificação de correção do software, podendo-se constatar que não há uma técnica amplamente aceita, que seja capaz de provar essa correção (GARRET; APOSTOLAKIS, 1999).

Pode-se pensar na possibilidade de se efetuar o teste exaustivo de um software de maneira a se verificar seu comportamento em todos os caminhos existentes em seu código, o que, na prática, é inviável devido ao enorme número de estados que um software (mesmo não muito sofisticado) pode assumir.

Outra linha aponta para a utilização de técnicas de prova formais. Estas técnicas ainda não atingiram um estágio considerado aceitável para um amplo uso, sendo utilizadas apenas em pequenos trechos de programas, devido à complexidade de sua aplicação. O grande problema se refere ao treinamento adequado da equipe técnica.

Um ponto a ser considerado é a realização de um projeto de software robusto, ou seja, software que, mesmo na presença de erros, seja capaz de evitar condições perigosas, ou seja, ser tolerante a falhas (BROOMFELD; CHUNG, 1997).

Não é apenas no software que devem existir mecanismos de tolerância a falhas, mas também no hardware de Sistemas Críticos. Em ambos os casos é fundamental que se detecte a ocorrência de falhas, permitindo que os mecanismos de tolerância a falhas possam ser acionados (VOAS, 2001).

No início de um projeto de um Sistema Crítico, faz-se a divisão entre o que deverá ser implementado por componentes programáveis e o que deverá ser implementado por componentes não programáveis. Essa escolha tem sua justificativa, pois determinados tipos de aplicações ainda não aceitam sistemas totalmente computadorizados. Dessa forma, as partes mais vitais do circuito são implementadas por meio de componentes mais tradicionais e de confiabilidade plenamente demonstrada em dezenas ou centenas de projetos similares. No caso de componentes programáveis também deve ser feira outra escolha, que é entre a implementação de determinadas funções por hardware ou por software.

Em Sistemas Críticos, a escolha da tecnologia e das soluções de projeto é diferente de sistemas convencionais, onde o custo desempenha, normalmente, papel primordial. Em Sistemas Críticos não é viável a seleção de uma opção de menor custo em detrimento da Segurança Crítica do sistema.

Na medida do possível, o projeto deve ser feito de forma hierárquica, projetando-se a arquitetura de tal forma que os módulos críticos estejam nos níveis mais baixos, sendo conveniente que tais componentes contenham a maior parte ou se possível todas as funções de Segurança Crítica do Sistema Crítico. Tal forma de projeto mostra-se adequada porque reduz o número de blocos ou módulos diretamente relacionados com a Segurança Crítica do sistema. Esses módulos diretamente relacionados com a Segurança Crítica são os que devem merecer maior atenção e cuidado em seu projeto. Os demais módulos também devem ser projetados com as melhores técnicas, mas seu nível de exigência é menor, pois em caso de falha, os módulos dos níveis inferiores garantirão a Segurança Crítica do sistema.

Uma das formas de se implementar a Segurança Crítica é através de mecanismos de intertravamento, cuja finalidade é assegurar que ações potencialmente inseguras sejam realizadas apenas em momentos em que elas não tenham possibilidade de causar acidentes, como por exemplo, levantar uma cancela em um cruzamento ferroviário não é inseguro, se não houver trem se aproximando do mesmo.

A manutenção do Sistema Crítico já deve ser prevista e programada desde o início do projeto. Se o projeto já for feito de forma a prever um processo de manutenção apropriado, as tarefas dessa etapa serão simplificadas e realizadas de forma mais adequada.

Existem dois tipos de manutenção a serem realizados, a manutenção preventiva e a manutenção corretiva. A manutenção preventiva tem como finalidade manter o sistema em bom estado, removendo efeitos de desgaste e envelhecimento, antes que possam resultar em falhas. O projeto pode prever que a manutenção seja feita com o sistema em funcionamento ou então exigir seu desligamento para que a manutenção possa ser feita. A manutenção corretiva visa fazer com que o sistema retome seu estado normal de operação após a ocorrência de algum tipo de falha. Em sistemas

tolerantes a falhas, o reparo pode ser feito imediatamente após a detecção do problema ou em um momento posterior, mais conveniente.

2.4.1. Modos de Falha de Sistemas Críticos

Modos de falha representam situações em que há falhas no Sistema Crítico, seja por falhas ocorridas nos componentes de hardware, ou mesmo em seu projeto, seja por falhas na especificação, projeto ou ainda na codificação do software.

A análise dos modos de falha de um circuito integrado de alta escala de integração é uma tarefa de extrema complexidade, bem como determinar seus efeitos em um Sistema Crítico.

Em sistemas deste tipo pode-se dividir as falhas que ocorrem em falhas detectáveis e não detectáveis. As falhas detectáveis são aquelas que o próprio Sistema Crítico consegue observar sua ocorrência, sinalizando tal fato e permitindo que se executem as devidas ações corretivas. Falhas não detectáveis são aquelas não percebidas pelos mecanismos de detecção e que permanecem residentes no Sistema Crítico.

Outra classificação das falhas que ocorrem em Sistemas Críticos relaciona-se aos efeitos que tais falhas possam acarretar. Se as conseqüências forem inseguras, a falha é dita como sendo insegura. Por outro lado, se as conseqüências não provocarem situações inseguras, a falha é classificada como sendo segura.

Tendo em vista essas duas formas de classificação, pode-se agora esclarecer um aspecto de fundamental importância, referente às falhas não detectáveis e inseguras, problema este que ganha importância maior pelo fato de se estar trabalhando com circuitos integrados de alta escala de integração.

Um sistema implementado através de uma arquitetura tolerante a falhas, normalmente supõe a existência de módulos redundantes. A ocorrência de uma falha do tipo inseguro e não detectável em um dos módulos da arquitetura permanece no sistema sem, no entanto, causar situações inseguras, pelo menos em um primeiro momento. Por outro lado, podem ocorrer falhas compensatórias em outros módulos, ou seja, falhas que afetem o funcionamento dos demais módulos do sistema da mesma forma que a falha insegura do primeiro módulo. Desta forma, o dispositivo

comparador da saída de cada módulo irá ser induzido a produzir saídas incorretas, gerando condições inseguras para o Sistema Crítico. Se este não dispuser de módulos redundantes, a falha inicialmente descrita, por si só, já será capaz de produzir estados inseguros no Sistema Crítico.

No entanto, há uma consideração que ameniza o impacto das falhas não detectáveis e inseguras no sistema. Os circuitos integrados com alta escala de integração possuem altas taxas de falhas, quando comparados com componentes convencionais e mesmo circuitos integrados com pequena e média escalas de integração. No entanto, apenas uma pequena parcela dessa taxa de falhas refere-se a situações que irão provocar estados inseguros no sistema. Isto ocorre porque a maioria das falhas acaba por desabilitar completamente o funcionamento de um circuito integrado, e apenas uma parcela mínima dessas falhas irá, de fato, estabelecer condições inseguras no Sistema Crítico.

Dessa forma, se a taxa de falhas insegura for considerada igual à taxa de falhas integral do circuito integrado, o Tempo Médio para uma Falha Insegura - MTTUF (*Mean Time To Unsafe Failure*) resultante seria extremamente pessimista, pois estaria considerando valores muito altos das taxas de falhas como inseguros. A taxa de falhas integral representa o valor diretamente obtido de normas, valor esse que considera todas as falhas verificadas em um circuito integrado, venham tais falhas a provocar ou não situações inseguras.

Considerando-se o emprego de componentes com alta escala de integração, pode-se dizer que os valores utilizados como suas taxas médias de falhas, devem sofrer uma redução, através de um determinado fator (CAMARGO et al., 2001).

A maioria dos modos de falha de um processador é seguro e não leva o sistema a um estado inseguro, especialmente se forem implementados sinais dinâmicos para a geração de saídas. Isto significa que, para que seja feita a liberação de uma determinada saída, o sinal deve possuir uma característica dinâmica, ou seja, ter uma freqüência diferente de zero. Assim, na ausência de alternância no sinal de saída, esta é considerada como inativa. Tal forma de implementação constitui uma prevenção contra sinais presos ao nível “zero” ou ao nível “um”, situações de ocorrência

bastante comum em um cartão eletrônico que contenha circuitos integrados, principalmente circuitos complexos.

Finalizando este item sobre modos de falhas, pode-se dizer que as falhas mais significativas identificadas para o processamento de sinais em Sistemas Críticos, sejam elas provocadas pelo hardware ou pelo software são (ALMEIDA, 1999):

- Obtenção de sinais de entrada com valores inconsistentes ou não esperados;
- Não obtenção de sinais de entrada ou chegada de excessivo número de sinais de entrada em um determinado período de tempo;
- Obtenção de sinais de entrada fora de sincronismo entre si ou com outros sinais internos;
- Incapacidade de tratar adequadamente a quantidade de sinais de interrupção gerados;
- Obtenção de sinais de entrada ou geração de sinais de saída com valores fora do intervalo de tempo especificado, ou ainda, não geração de sinais de saída especificados;
- Uso incorreto de constantes e variáveis ou ocorrência de condições de *overflow* ou de *underflow* no processamento;
- Utilização imprópria de áreas de memória ou ocorrência de invasão da área de memória reservada à pilha do programa;
- Existência de laços sem fim ou ocorrência de condição de *deadlock* no programa;
- Erro na passagem de parâmetros entre rotinas ou duração excessiva na execução de uma rotina.

2.4.2. Formas de Implementação de Redundância

A forma mais utilizada para a prevenção dos efeitos de falhas em Sistemas Críticos é a utilização de módulos redundantes. Há quatro formas para que se faça implementação de redundâncias em um Sistema Crítico, que são a redundância de hardware, de software, de informação e redundância temporal (STOREY, 1996).

A Redundância de Hardware implica na inclusão de circuitos de hardware adicionais ao mínimo necessário para o funcionamento do sistema. A Redundância de Software implica na geração de versões distintas do software do sistema ou de partes desse software, sempre se baseando em uma especificação comum.

A Redundância de Informação implica na inclusão de informação adicional àquela estritamente necessária ao funcionamento do sistema, como por exemplo bits de paridade, códigos de detecção e correção de erros e *checksums*, dentre outros.

Por fim, a Redundância Temporal consiste na repetição de cálculos e a comparação de seus resultados, possibilitando a detecção de possíveis falhas transientes e intermitentes no hardware.

Cada uma dessas formas de implementação de redundância é descrita, de maneira detalhada, nos próximos itens.

2.4.3. Redundância de Hardware

O emprego de redundância em um Sistema Crítico consiste na utilização de componentes auxiliares com a finalidade de realizar as mesmas funções desempenhadas por outros elementos presentes no sistema. A finalidade principal da utilização de redundância nesses sistemas é a prevenção de condições ou estados inseguros.

Embora a redundância sempre implique na adição de novos componentes, deve-se fazer o possível para não aumentar a complexidade do sistema, de forma a não se ter efeito contrário, ou seja, diminuição da confiabilidade e da segurança do sistema.

A redundância de hardware pode ser implementada através de três formas básicas (JOHNSON, 1989):

- Redundância Estática: utiliza o mascaramento de falhas como principal técnica e o projeto é feito de forma a não requerer ações específicas do sistema ou de sua operação em caso da ocorrência de falhas;

- Redundância Dinâmica: implica na detecção de falhas, caso em que o sistema deve tomar alguma ação para anular seus efeitos, o que normalmente envolve uma reconfiguração do sistema;
- Redundância Híbrida: consiste na combinação de técnicas estáticas com técnicas dinâmicas. Utiliza mascaramento de falhas para prevenir que erros se propaguem, detecção de falhas e reconfiguração para remover, do sistema, unidades com falha.

2.4.3.1. Redundância Estática

As técnicas de redundância estática apóiam-se no uso de um mecanismo de comparação, que compara as saídas de um determinado número de módulos, mascarando o efeito de falhas nesses módulos. A arquitetura mais simples da redundância estática é a que utiliza dois módulos redundantes com um circuito comparador na saída desses módulos. Um estágio posterior é o que utiliza três módulos redundantes com um circuito de votação na saída dos mesmos. Maior grau de tolerância a falhas é obtido com o uso de módulos redundantes adicionais.

a) Dois Módulos com Comparação

Na arquitetura duplicada com comparação, apresentada na figura 2.3, são utilizados dois módulos ou canais redundantes. Cada módulo recebe as mesmas entradas e deve executar as mesmas funções, segundo uma mesma especificação. O desejável é que cada canal seja implementado independentemente, ou seja, com hardware e software distintos, aumentando a independência entre eles e diminuindo a possibilidade de ocorrência de falhas comuns aos dois canais.

As saídas de cada módulo são enviadas a um circuito comparador que, em caso de desacordo das saídas dos dois canais, deve ter um procedimento que gere um valor considerado seguro ao Sistema Crítico. Se houver igualdade entre os sinais das saídas dos dois canais, é esse mesmo sinal que será passado à saída do sistema de controle.

Este tipo de arquitetura não é considerado como tolerante a falhas, visto que na maioria dos casos, quando ocorre a falha de um módulo, o Sistema Crítico é desativado, e a Aplicação Crítica é levada a um estado seguro. No entanto, quando houver desacordo nas saídas dos módulos, pode-se selecionar um dos módulos como o mais confiável, caso em que se estará utilizando uma forma de tolerância a falhas.

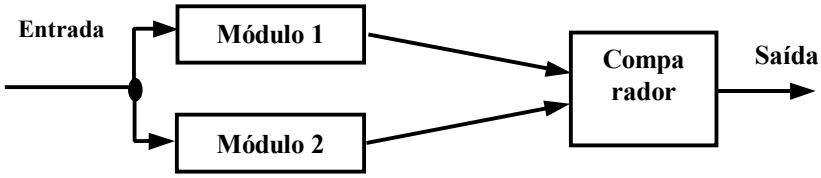

Figura 2.3 – Arquitetura com Dois Módulos Redundantes

b) Três Módulos com Votação - Redundância Modular Tripla

Na arquitetura com redundância modular tripla - TMR (*Triple Modular Redundancy*), apresentada na figura 2.4, utilizam-se três módulos que desempenham funções idênticas, com um circuito na saída, cuja função é a de votação dos sinais de saída de cada módulo. Se, por uma falha, a saída de um módulo diferir das saídas dos outros dois módulos, o votador gera a saída com base no resultado da maioria dos módulos, ou seja, dos dois módulos sem falha. Portanto, esta arquitetura tolera uma falha simples em um dos módulos. Da mesma forma que no caso de dois canais com comparação, se houver igualdade entre os sinais nas saídas dos três canais, esse é o sinal a ser passado à saída.

De maneira similar à duplicação com comparação, o ideal é que cada módulo tenha implementação distinta dos demais, eliminando erros comuns que possam ter permanecido no projeto dos módulos.

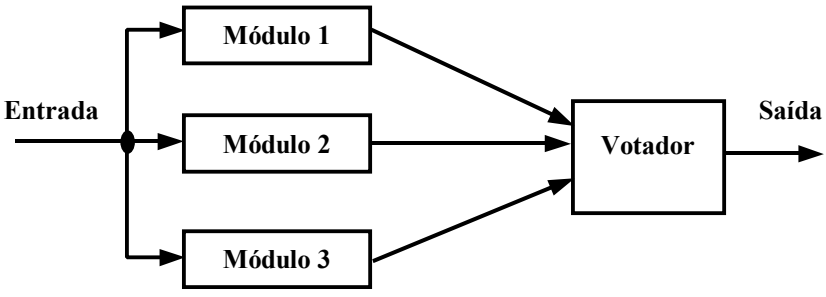

Figura 2.4 – Arquitetura com Três Módulos Redundantes

Os pontos fracos das arquiteturas com dois e três módulos redundantes são:

- As entradas normalmente provêm de um único sensor, que também pode apresentar falha. Uma solução é também duplicar ou triplicar o número de sensores dos sinais de entrada;
- Os circuitos comparador e votador são únicos e não implementam tolerância a falhas. Portanto, esses circuitos devem ser implementados de forma mais elaborada, e se possível, usando tecnologia *fail-safe* que, no caso de qualquer falha, leve o sistema a um estado conhecidamente seguro;
- No caso da arquitetura TMR, após a falha em um módulo, o sistema perde a habilidade de tolerar falhas, pois uma falha similar em um segundo módulo pode gerar uma situação insegura. A solução é dotar o sistema de meios de detecção de falhas, gerando avisos ou alarmes para que o módulo com falha seja reparado ou substituído.

c) Redundância N-Modular

Podem ser utilizadas extensões da arquitetura TMR, fazendo-se uso de cinco ou até sete processadores, votando-se as respectivas saídas de cada módulo. Essa extensão da arquitetura TMR recebe a denominação de *N-Modular Redundancy* – NMR, sendo apresentada na figura 2.5.

Esta arquitetura tolera (N - 1)/2 módulos com falhas. Por exemplo, em uma arquitetura com cinco módulos, toleram-se falhas em até dois módulos.

As desvantagens em se aumentar o número de módulos estão no aumento de custo e de complexidade, sem considerar outros fatores como o maior volume e peso do equipamento e seu maior consumo de energia.

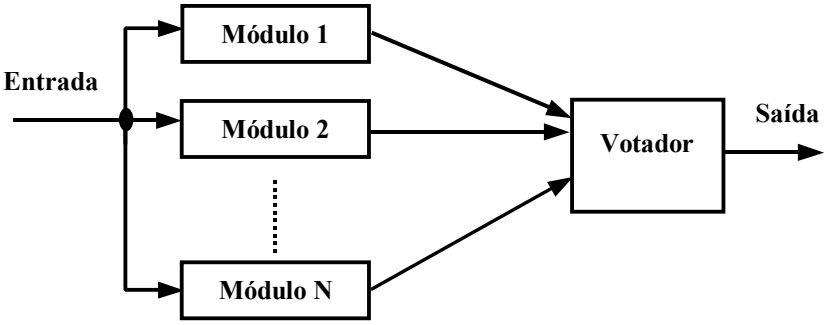

Figura 2.5 – Arquitetura Redundante NMR

2.4.3.2. Redundância Dinâmica

Neste tipo de arquitetura, há, normalmente, um módulo em operação e um ou mais módulos em espera (*standby*), que devem entrar em operação quando o módulo inicial apresentar falha. Este tipo de arquitetura reduz a redundância necessária, mas sua segurança depende diretamente da capacidade em se detectar falhas. Tolera-se um módulo com falha se houver apenas dois módulos presentes no sistema, tolerando-se dois módulos com falha se houver três módulos no sistema, e assim por diante.

Esta arquitetura é mais apropriada a sistemas que tolerem erros temporários de operação, pois às vezes uma falha só é detectada após ter produzido algum efeito não desejado nas saídas.

a) Módulo Reserva em Espera (*Standby*)

Este tipo de arquitetura é mostrado na figura 2.6. No funcionamento sem falha, o módulo 1 está em operação e o módulo 2 em espera. O detector de falhas indica ao circuito de chaveamento qual módulo deve ser o responsável pela geração das saídas.

Na ocorrência de falha no Módulo 1, o Detector de Falhas sinaliza ao módulo de Chaveamento para que este faça a substituição do Módulo 1 pelo Módulo 2, de forma que a geração das saídas continue sendo feita corretamente. Se o módulo em espera estiver processando as entradas, simultaneamente, ao módulo principal (*hot standby*), tem-se uma agilização do processo de substituição. Esse processo é vital em sistemas que não podem tolerar interrupções significativas de processamento (ESSAMÉ et al., 1997). Caso contrário, se o módulo em espera não estiver realizando nenhuma tarefa (*cold standby*), o tempo de substituição de módulos será maior.

Este tipo de arquitetura pode ser expandido para N módulos, ficando N – 1 módulos em espera. O sucesso deste tipo de arquitetura depende de uma correta implementação do Módulo Detector de Falhas, que é o responsável direto pela detecção de falhas e por sua indicação para o chaveamento das saídas.

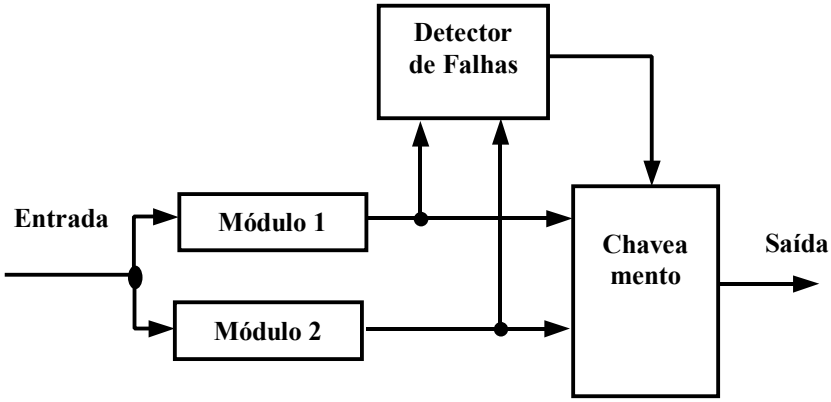

Figura 2.6 – Arquitetura com Módulo Reserva em Espera

b) *Self Checking*

Constitui-se em uma variante da técnica Módulos Reserva em Espera. A saída de um dos módulos é a saída do sistema e a saída do comparador é utilizada para a detecção e sinalização de falhas, conforme mostra a figura 2.7. Esta técnica também se constitui em uma variante da arquitetura com dois módulos com comparação.

Ambos sinais, de saída e de detecção de falhas são enviados à Aplicação Crítica. Se o sinal de detecção indicar a ocorrência de problemas, a aplicação deve prever mecanismos de prevenção de situações perigosas.

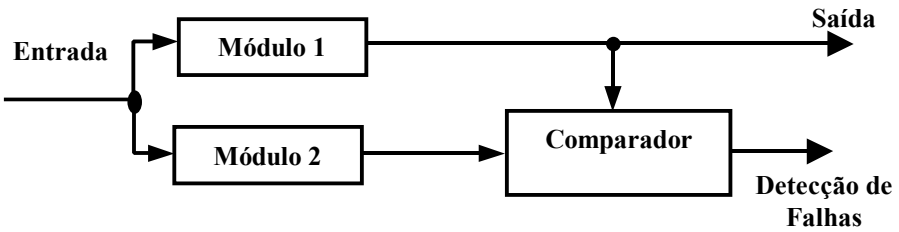

Figura 2.7 – Arquitetura *Self Checking*

2.4.3.3. Redundância Híbrida

Este tipo de arquitetura representa uma combinação das técnicas de votação, detecção de falhas e chaveamento de módulos. O nome mais comumente atribuído a esta técnica é Redundância N-Modular com Módulos Reserva.

Esta arquitetura é ilustrada na figura 2.8. No início, os N módulos principais estão ativos e os sinais de suas saídas chegam ao votador, cujo funcionamento é similar ao já descrito. Quando um dos módulos principais falhar, apresentando valor de saída diferente dos demais, tal fato é indicado pelo Detector de Desacordo, que providencia sua sinalização ao Chaveador. Este, por sua vez, providencia a substituição do módulo com falha por um dos módulos reserva. Desta forma, reúne-se a tolerância a falhas com a reconfiguração do sistema.

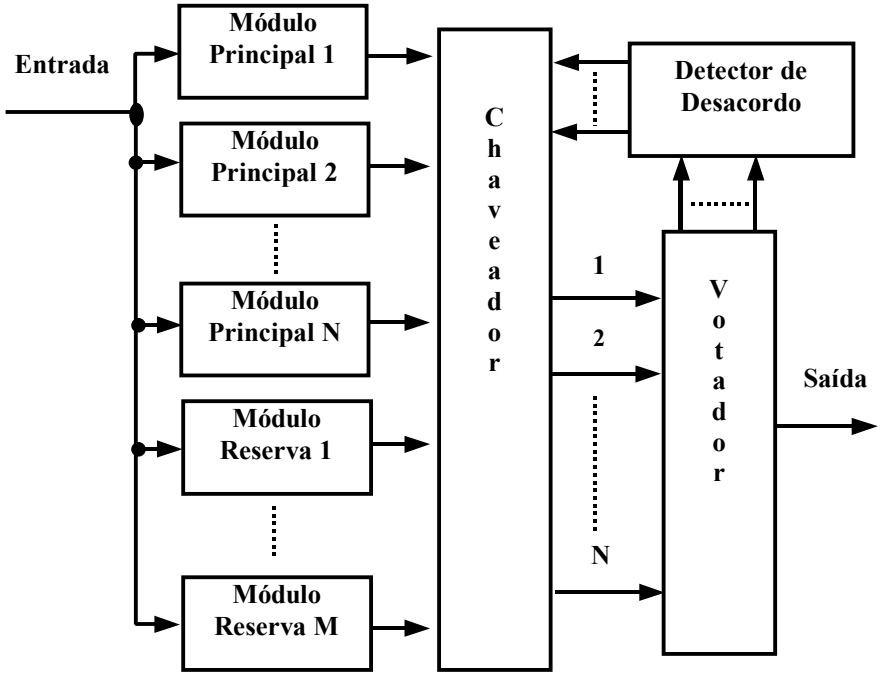

Figura 2.8 – Redundância N-Modular com Módulos Reserva

2.4.4. Redundância de Software

O grande problema em relação aos sistemas que envolvem segurança e que têm o software como componente crítico está na ausência de uma metodologia de eficiência reconhecida para a avaliação de sua segurança e, conseqüentemente, de seu reflexo dentro dos níveis de risco aceitáveis de um Sistema Crítico. Um primeiro aspecto é estabelecer os níveis de risco aceitáveis, que dependem de cada tipo de aplicação, enquanto que o segundo ponto consiste em como demonstrar que tais níveis de risco vêm sendo atendidos, principalmente quando se envolve software.

Pode-se dizer que a falta de completeza das especificações de software e das especificações em relação ao ambiente de aplicação representa um grave problema, fazendo com que o sistema atinja situações imprevistas, como conseqüência de procedimentos operacionais incorretos, de mudanças não esperadas no ambiente operacional, ou ainda de modos de falhas não previstos do sistema (JAFFE et al., 1991).

Um possível caminho para se definir e avaliar melhor o conceito de segurança é através da definição de um conjunto de fatores que consigam representar adequadamente o conceito de segurança (KITCHENHAM; PELEEGER, 1996).

2.4.4.1. Software para Sistemas Críticos

Em função da dificuldade da comprovação da não existência de falhas na implementação de um software, em relação à sua especificação, são utilizadas técnicas de redundância de software, cujo objetivo é tornar o software mais robusto em relação à segurança, ou seja, tolerante a falhas porventura ainda existentes (JOHNSON, 1989).

Quando um hardware é replicado, há a proteção contra falhas aleatórias em seus componentes. O mesmo não ocorre com o software, visto que qualquer problema irá afetar igual e simultaneamente (se houver processamento paralelo) todos os módulos. Daí a necessidade em se diversificar as versões do software. No que se refere à redundância de software, há duas alternativas principais, que são a utilização de N-Versões e o Bloco de Recuperação (BURNS; WELLINGS, 1997).

a) Programação N-Versões

A programação N-Versões tem sua origem no hardware NMR. O software não se desgasta e o foco principal está na detecção de falhas de projeto. Devem ser geradas N versões de um programa, que executem as mesmas funções, a partir de uma mesma especificação, proporcionando diversidade de projetos (KELLY et al., 1991). Os programas são executados, concorrentemente, a partir das mesmas entradas e seus resultados são comparados. Na figura 2.9 é ilustrado o caso com três versões de software. Em princípio, os resultados deveriam ser os mesmos, o que pode não ocorrer, proporcionando a detecção de falhas de programação em algumas das versões. Supõe-se que falhas em uma versão sejam independentes das demais versões. Cada versão pode ser executada de maneira seqüencial, no mesmo processador, ou em paralelo, em processadores distintos.

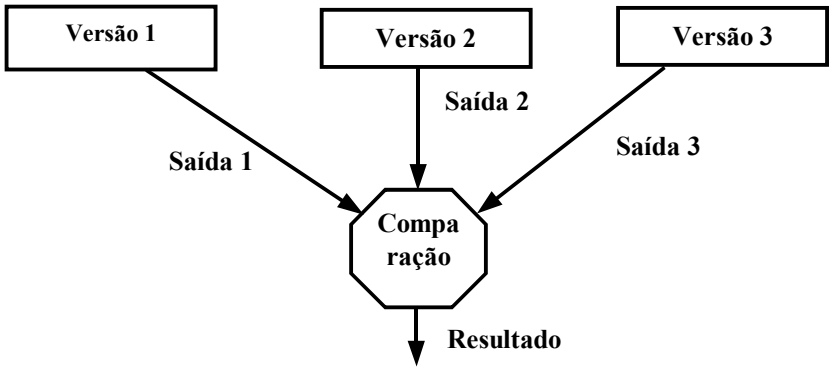

Figura 2.9 – Programação N-Versões

No caso de haver desacordo entre as saídas, há pelo menos quatro opções a serem seguidas, que são executar um novo processamento, reiniciar o sistema, realizar uma transição para um estado previamente definido ou depositar maior confiança no resultado de uma das versões.

O sucesso desta técnica depende de uma especificação inicial correta, pois um erro na especificação irá se propagar por todas as versões. Também é necessário que se tenha independência entre as equipes de projeto, de forma a se evitar erros comuns entre as versões do programa. O orçamento para o desenvolvimento de mais de uma versão é muito mais alto e o desenvolvimento será mais demorado para se produzir e

manter N versões distintas que executem as mesmas funções, no lugar de se ter apenas uma versão em execução em todos os processadores.

Se as N versões forem executadas em uma mesma máquina, há o problema da multiplicação do tempo total de processamento por um fator maior do que N, considerando-se aí o tempo para a votação ou para a comparação dos valores de saída.

b) Bloco de Recuperação

A técnica do Bloco de Recuperação é um tipo de redundância dinâmica, conforme mostra a figura 2.10. Estes blocos são implementados apenas para as seções críticas do software. Nestes casos, entra-se em um Bloco de Recuperação, através de seu ponto de entrada (Entrada do Bloco de Recuperação). São executados um a um os blocos alternativos até que, no teste de aceitação, seja obtido um resultado dentro das expectativas ou de padrões pré-estabelecidos. Se, após todos os blocos alternativos tiverem sido executados e testados, não tiver sido obtido um resultado dentro das expectativas ou de padrões pré-estabelecidos, ocorre a falha do bloco, caso em que alguma ação preventiva e/ou corretiva deve ser tomada.

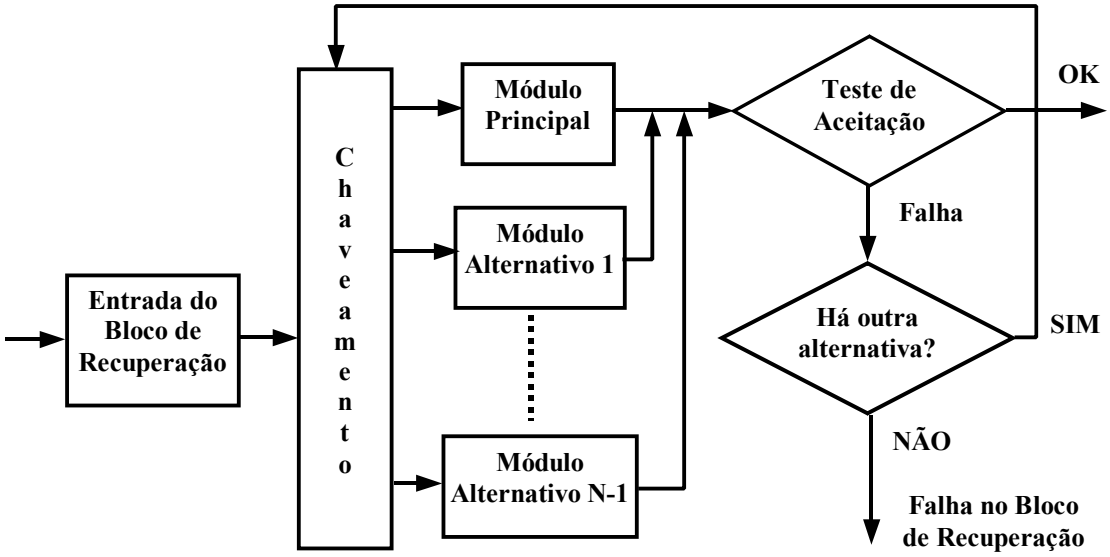

Figura 2.10 – Bloco de Recuperação

Esta técnica também apresenta problemas de custos adicionais de desenvolvimento de algoritmos alternativos.

2.4.4.2. Processo de Desenvolvimento de Software para Sistemas Críticos

Os princípios gerais de projeto recomendados para o desenvolvimento de software de Sistemas Críticos são incluir procedimentos que aumentem a segurança, sem aumentar sensivelmente a complexidade do programa, bem como propiciar maiores facilidades para a certificação de seu funcionamento.

O software contribui para a ocorrência de condições perigosas, tanto pela omissão (falha em fazer algo requisitado), quanto por executar alto que não deveria ser realizado ou ainda, por fazê-lo no momento errado ou na seqüência incorreta.

O processo de desenvolvimento de software para Sistemas Críticos reveste-se de grande importância, tendo em vista seu papel vital nesse tipo de sistemas. Segundo a norma EN 50128 (CENELEC, 1998b) as principais etapas no processo de desenvolvimento de um software para Sistemas Críticos são: especificação de requisitos, projeto da arquitetura, projeto dos módulos, testes, integração dos módulos e integração com o hardware do sistema.

Na etapa de especificação de requisitos devem ser detalhados alguns aspectos como a funcionalidade do software, incluindo a capacidade de processamento e os tempos de resposta necessários. Ainda nesta etapa devem ser especificadas as funções diretamente ligadas à Segurança Crítica, bem com seus Níveis de Integridade de Segurança. Outros aspectos a serem especificados são a questão da usabilidade do sistema, suas interfaces com o ambiente externo, seus modos de operação e as principais restrições existentes.

Em relação à especificação, existem abordagens realizadas através de métodos formais, com notação matemática, e através de métodos não formais, baseados, fundamentalmente, em técnicas de modelagem.

Os métodos com enfoque formal englobam a geração de especificações através métodos que utilizam notações matemáticas, tais como VDM (Viena Development Method) e Z (WILLIAMS, 1994).

Os métodos formais mostram-se mais apropriados quando aplicados por equipes com pequeno número de pessoas, sendo importante que sejam profissionais com boa experiência nas fases de especificação, modelagem e análise de Sistemas de Críticos. No entanto, sua aplicação é inadequada quando realizada por uma equipe grande com profissionais inexperientes na captura dos requisitos (BROOMFIELD; CHUNG, 1997).

Na etapa de projeto da arquitetura do software, constitui um ponto importante a interação do software com o hardware, considerando-se o nível de integridade (SIL) de cada módulo. Se forem utilizadas ferramentas comerciais de prateleira de software (COTS – *Comercial Off-The Shelf*) em sistemas de nível de integridade 3 ou 4, deve ocorrer um processo de análise dessas ferramentas. Finalmente, deve-se procurar minimizar a porção do software responsável pela Segurança Crítica.

No projeto dos módulos de software, os objetivos são de minimizar o tamanho e a complexidade de cada módulo, especificar as interfaces do módulo com o ambiente e com outros módulos. Deve-se ainda descrever a estrutura de dados empregada, além dos principais algoritmos. A linguagem utilizada deve possuir características que facilitem a identificação de falhas na codificação.

Na parte relativa aos testes e à integração entre módulos de software e entre software e hardware devem ser detalhados os casos de teste a serem realizados, o ambiente em que os testes devem ser efetuados, quais as ferramentas a serem utilizadas, qual a configuração a ser empregada, bem como os critérios de correção a serem adotados.

2.4.5. Redundância de Informação

A Redundância de Informação corresponde à adição de informação, para permitir a detecção, o mascaramento e, possivelmente, a tolerância a falhas (JOHNSON, 1989), (SIEWIOREK, 1982). O objetivo da redundância de informação é garantir a consistência dos dados obtidos e utilizados em Sistemas Críticos, de forma a detectar eventuais falhas decorrentes de problemas no hardware, como eventuais interferências eletromagnéticas.

Um conceito importante é a distância de Hamming, que representa o número de bits distintos entre duas palavras de código. Por exemplo, as palavras de código 0000 e 0101 diferem em duas posições, e portanto têm uma distância de Hamming igual a 2. Outro conceito utilizado é a distância de código, que representa a distância mínima de Hamming entre duas palavras de código.

Basicamente, em sistemas computacionais, a redundância de informação tem por objetivo aumentar a distância de código entre palavras de código válidas, através da introdução de bits de redundância. Para se aumentar essa distância de código, deve-se, conseqüentemente, aumentar a quantidade de informação no código válido, originando, dessa forma, um novo código. As informações adicionadas podem estar entrelaçadas ou não ao código original. Se não estiverem, o código é dito separável; caso contrário, é denominado não-separável. O processo de codificação e decodificação é mais complexo quando se trata de um código não separável.

As principais técnicas utilizadas na redundância de informação são as seguintes (JOHNSON, 1989):

- Código de Paridade: compreende a adição de um bit a cada palavra. O bit adicional é calculado como o total de bits com valor “1” na palavra. Se o número de bits “1” da palavra for par, e a paridade escolhida for par, o bit adicional deverá ter o valor “0”. Similarmente, se o número de bits “1” da palavra for impar, e a paridade escolhida for par, o bit adicional deverá ter o valor “1”.

- Códigos m de n: consiste em códigos com palavras contendo comprimento total de **n** bits, sendo que desses **n** bits, exatamente **m** deverão conter o valor "1". Por exemplo, um código **3 de 6** significa um código de comprimento total de **6** bits, contendo exatamente **3** bits "1";
- Códigos Duplicados: consiste na duplicação do código original. Apresenta a vantagem de ter implementação simples, e a desvantagem de ter um grande número de bits adicionais;
- *Checksums*: consiste na somatória dos dados originais, sendo tal somatória agregada ao grupo de palavras em questão;
- Códigos Cíclicos: é obtido por meio da utilização de um polinômio gerador (**G(x)**) de grau igual a **n – R**, onde **n** é o número de bits contidos na palavra codificada por **G(x)** e **R** é o número de bits na informação original a ser codificada.

2.4.6. Redundância Temporal

Este tipo de redundância consiste em se realizar o processamento necessário mais de uma vez. O processamento adicional pode ser realizado a partir da consideração de duas condições.

A primeira é o caso em que são coletados valores das variáveis de entrada em dois ou mais instantes de tempo, utilizando-se tais valores em pelo menos duas execuções do respectivo código.

A segunda é o caso em que o correspondente código é executado mais de uma vez, aproveitando-se as mesmas entradas. As diversas execuções são capazes de detectar erros oriundos de falhas transientes e intermitentes do hardware, uma vez que falhas permanentes irão resultar nos mesmos valores, em quantas execuções do código sejam realizadas.

De forma a manter a Segurança Crítica em Sistemas de Críticos, além de uma boa técnica de implementação, faz-se necessária a realização de uma Análise de Segurança dos projetos, sempre com o objetivo de manter, em níveis aceitáveis, a

segurança de sistemas e aplicações. Portanto, no próximo item é descrita uma metodologia de Análise de Segurança desses sistemas.

2.5. Análise de Segurança de Sistemas Críticos

A Análise de Segurança de Sistemas de Críticos tem uma importância primordial no aspecto de verificar se os requisitos de Segurança Crítica, descritos na especificação de requisitos do sistema, são atendidos. É importante destacar que, em certos níveis de criticidade dos sistemas, as equipes de desenvolvimento e de Análise de Segurança devem ser independentes entre si, seja do ponto de vista técnico, seja do aspecto financeiro.

Uma das atividades realizadas na Análise de Segurança é verificar se mecanismos adequados de Segurança Crítica estão presentes no Sistema Crítico. Outras atividades são identificar situações de falha que, isoladas ou em combinação, possam levar a um acidente, bem como determinar possíveis efeitos de danos resultantes de condições perigosas. Outros objetivos da Análise de Segurança são a identificação de critérios de projeto e de dispositivos de segurança ou mesmo procedimentos que possam eliminar ou minimizar perigos.

2.5.1. Análise Qualitativa e Análise Qualitativa

Há duas formas principais para se efetuar uma Análise de Segurança, que são a análise do tipo qualitativo e a análise do tipo quantitativo. Antes que se possa obter valores numéricos, através de uma análise quantitativa, é indispensável a realização de uma análise qualitativa eficiente, sem a preocupação de se atribuir valores às ocorrências. Uma análise quantitativa não deve desviar o foco dos problemas existentes, tais como falhas de projeto. Uma das principais utilidades deste tipo de análise é se fazer uma comparação entre sistemas com funções similares (The CHANNEL, 1994).

A Análise Qualitativa procura identificar mecanismos que implementem os requisitos especificados, de forma que se mantenha o nível de segurança de um Sistema Crítico durante sua operação (SEAMAN, 1999).

Já a Análise Quantitativa procura medir a probabilidade do sistema atingir um estado inseguro. Neste sentido, a maior contribuição do software utilizado em Sistemas Críticos refere-se à melhoria no fator de cobertura de falhas, através de rotinas de detecção e recuperação de falhas. Este aspecto pode influenciar diretamente na modelagem final da segurança do sistema sob avaliação.

No próximo item descreve-se uma metodologia de Análise de Segurança que contempla esses dois tipos de avaliações.

2.5.2. Metodologia de Análise de Segurança

Em um Sistema Crítico é de grande importância a realização de atividades de Análise de Segurança. A metodologia de análise de segurança seguida dentro do Grupo de Análise de Segurança do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da USP, do qual o autor é um de seus coordenadores, é composta por algumas etapas. Essas etapas são a Determinação dos Requisitos Gerais de Segurança, Mapeamento dos Requisitos Gerais de Segurança, Análise dos Módulos Responsáveis pela Segurança e Avaliação do Grau de Segurança (CAMARGO; ALMEIDA, 1999). A figura 2.11 apresenta a interconexão existente entre as etapas desta metodologia, detalhadas a seguir.

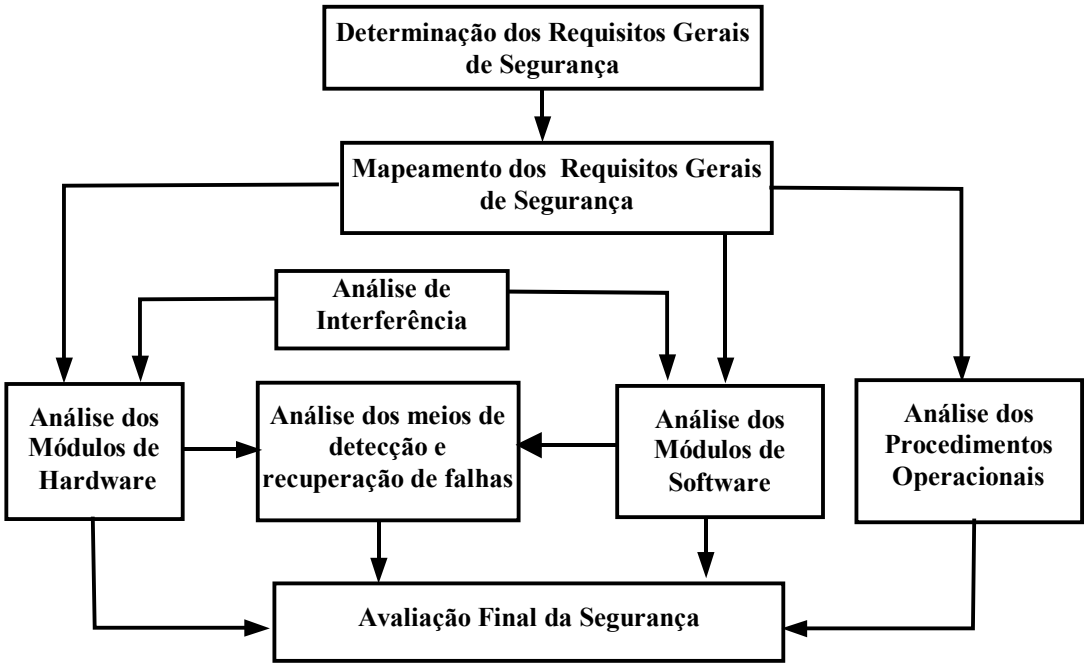

Figura 2.11 - Etapas da Metodologia de Análise de Segurança

a) Determinação dos Requisitos Gerais de Segurança

Os Requisitos Gerais de Segurança constituem-se em regras que o controle do sistema não pode violar, sob o risco de provocar uma situação perigosa. Portanto, a determinação desses requisitos trará impactos em todo o processo de análise, representando uma etapa de vital importância para todo o ciclo de análise. Para que os Requisitos Gerais de Segurança possam ser produzidos, faz-se necessário um entendimento do sistema em estudo. A partir daí é gerada uma Descrição Geral do Sistema Crítico e de sua arquitetura, sendo que tal descrição é finalizada com os Requisitos Gerais de Segurança.

Para que a identificação das situações potencialmente inseguras possa ser feita, é de grande importância a existência de interações com o operador do Sistema Crítico, cuja finalidade é a de se obter a maior quantidade possível de informações a respeito do sistema em análise.

b) Mapeamento dos Requisitos Gerais de Segurança

Nesta etapa é feito o mapeamento dos Requisitos Gerais de Segurança, ou seja, determinam-se quais os módulos componentes do Sistema Crítico em estudo, têm por atribuição garantir a segurança na operação, sejam eles componentes de hardware, software ou até mesmo procedimentos operacionais. Como conseqüência, podem ser determinados os Requisitos Específicos de Segurança para cada um dos módulos ou subsistemas. Esses requisitos específicos são obtidos pela decomposição dos requisitos gerais.

Para a adequada execução desta etapa, faz-se necessária a elaboração de um Relatório com a Descrição Detalhada do Sistema (Hardware, Software e Procedimentos Operacionais), que, além de auxiliar na determinação dos Requisitos Específicos de Segurança, fornecerá também os subsídios necessários para a próxima etapa da metodologia, ou seja, a análise propriamente dita.

c) Análise dos Módulos de Hardware

Neste item descrevem-se as atividades desenvolvidas na Análise de Segurança dos módulos de hardware. Inicialmente é realizada uma classificação do hardware em módulos *fail-safe* e redundantes.

Um módulo *fail-safe* é aquele em que uma falha sempre leva o módulo ou subsistema a um estado sabidamente seguro. Em um módulo ou subsistema implementado de forma redundante, utilizam-se dois ou mais circuitos ou programas que desempenham a mesma função.

Na análise dos módulos *fail-safe* são realizadas as seguintes atividades:

- Descrição Detalhada de Funcionamento em Operação Normal: descreve-se, de forma detalhada, o funcionamento dos circuitos, chegando-se ao nível da descrição da função de cada componente presente em cada circuito;
- Análise dos Modos de Falha dos Componentes: a partir da descrição em operação normal, analisam-se os circuitos, supondo-se a ocorrência de todos os modos de falha possíveis em cada um dos componentes dos circuitos. A essa técnica dá-se o nome de FMEA (*Failure Mode and Effect Analysis*); e
- Análise de Entradas Impróprias: também, a partir da descrição em operação normal, supõe-se a existência das chamadas entradas impróprias nos circuitos, como por exemplo, ruídos eletromagnéticos, temperatura excessiva, oscilação de fonte, etc. Realiza-se, então, uma nova análise supondo-se a ocorrência de cada uma destas entradas impróprias.

Na análise dos módulos redundantes são realizadas as seguintes atividades:

- Análise de Cada um de seus Subsistemas: utiliza-se o mesmo procedimento descrito para os módulos *fail-safe*;
- Análise de Independência de Cada Canal dos Módulos Redundantes: consiste na verificação da existência de falhas de modo comum que possam afetar todos os canais redundantes da mesma forma. Falhas de modo comum estão relacionadas, por exemplo, com fontes de alimentação e sinais de entrada.

d) Análise dos Módulos de Software

Nesta etapa procede-se à análise de todas as rotinas que constituem o software embutido no Sistema Crítico, seja a rotina responsável direta ou indiretamente por aspectos de Segurança Crítica. Este procedimento está ligado ao fato de que os módulos de software apresentam alto grau de dependência entre si.

As atividades que fazem parte desta etapa são:

- Preparação da documentação necessária de cada rotina, constituída por descrição funcional, diagrama estruturado ou fluxograma e casos de testes;
- Preparação da documentação necessária de cada variável e constante utilizada nas rotinas de software, composta por descrição das variáveis, rotinas que as lêem/modificam, estrutura de dados e estado inicial das variáveis;
- Inspeção do código fonte através da aplicação de uma lista de inspeção específica para cada linguagem de programação. Alguns dos itens verificados são: testes de entrada e saída de rotinas, teste de parâmetros, teste do fluxo de controle, etc.
- Reuniões entre os analistas envolvidos no trabalho, objetivando a análise das rotinas do sistema e a análise de interferência entre rotinas. Nestas reuniões nomeia-se um analista, para cada rotina, cuja incumbência é realizar a apresentação de seus aspectos funcionais. Os demais participantes da reunião têm como função realizar o questionamento da rotina, procurando identificar situações que possam levar o sistema a condições inseguras. Dentre os participantes desta reunião é importante a presença de, pelo menos, um profissional envolvido com a análise do hardware, cuja função é auxiliar no esclarecimento de questões relativas à implementação dos circuitos do Sistema Crítico. Essas reuniões não devem ter duração superior a duas 2 horas, visando manter a atenção de todos os participantes sobre os aspectos de Segurança Crítica do sistema.

e) Análise dos Mecanismos de Detecção e Recuperação de Falhas

Mecanismos de detecção de falhas são aqueles que permitem a identificação de módulos ou subsistemas com falha. São esses mecanismos que possibilitam a execução de procedimentos de substituição de módulos ou mesmo de reconfiguração do sistema. A análise e identificação desses mecanismos de detecção determinam o fator de cobertura de falhas existente no sistema, fornecendo subsídios para a etapa de Avaliação da Final da Segurança.

f) Análise dos Procedimentos Operacionais

Os procedimentos operacionais envolvidos são verificados, em conjunto com a análise dos módulos de hardware e de software. Esta verificação visa identificar seqüências operacionais que, eventualmente, possam levar o sistema a um estado potencialmente inseguro e que, portanto, devem ser evitadas.

g) Análise de Interferência

Considerando-se que há, normalmente, interfaces do Sistema Crítico com outros sistemas, pode ser que seja necessária uma análise parcial dos mesmos. A análise sobre tais sistemas deve estar centrada nos aspectos interferentes relativos a informações vitais do Sistema Crítico.

h) Avaliação Final da Segurança

Nesta etapa elabora-se um Relatório de Conclusões da Análise de Segurança, destacando-se:

- Software: apresentam-se os resultados obtidos na análise, destacando-se os problemas encontrados, de acordo com a seguinte classificação:
    - Rotinas que contêm problemas que não comprometem a segurança nem a disponibilidade do sistema;
    - Rotinas que contêm problemas que podem levar à ocorrência de anomalias operacionais e de disponibilidade; e
    - Rotinas que contêm problemas que podem levar o sistema a um estado potencialmente inseguro.

- Hardware: apresentam-se as conclusões da Análise dos Efeitos dos Modos de Falhas e das Entradas Impróprias para os módulos *fail-safe* e para os módulos redundantes, destacando-se as falhas ou entradas impróprias que podem levar o sistema a situações potencialmente inseguras.
- Sistema: apresenta-se o Grau de Segurança do sistema através do valor de seu Tempo Médio para Falha Insegura - MTTUF (*Mean Time To Unsafe Failure*), da sua confiabilidade através do valor de seu Tempo Médio Entre Falhas - MTBF (*Mean Time Between Failures*) e da influência dos procedimentos operacionais na segurança e na disponibilidade do sistema. Os cálculos realizados nesta etapa baseiam-se em modelos que representam a implementação do sistema em questão. Os modelos mais utilizados para estas avaliações são os Modelos Combinatórios (Série e Paralelo) e os Modelos de Markov.

Há outras formas de se realizar uma Análise de Segurança. Por exemplo, Reese e Leveson (1997) propõem uma metodologia de Análise de Segurança chamada *Software Deviation Analysis*, que é composta por uma variante automatizada da técnica HAZOP (HAZard and Operability Analysis). É vital que tal técnica seja aplicada ao longo do ciclo de desenvolvimento do software Tal método se baseia em especificações formais transformadas em diagramas que são comparados com possíveis desvios em relação ao funcionamento normal do sistema,

Tanto a implementação, quanto a Análise de Segurança de Sistemas Críticos baseiam-se em normas especialmente desenvolvidas para essas aplicações. Sendo assim, os principais aspectos de algumas dessas normas são descritos no item seguinte.

2.6. Normas Utilizadas em Aplicações Críticas

São vários os papéis que as normas desempenham na execução de um projeto, principalmente em Sistemas Críticos. Como exemplo, pode-se citar a função de auxílio à equipe de projeto, no sentido de garantir que o produto em desenvolvimento obedeça a um determinado nível mínimo de qualidade, bem como a função de seleção de métodos de projeto de eficiência reconhecida. Outras funções que podem ser citadas são promover uniformidade entre diversas equipes de trabalho, prover guias de projeto, além de proporcionar uma base legal no caso de disputas judiciais.

Para se certificar um sistema, normalmente, se faz necessária a utilização de normas apropriadas a cada aplicação. Algumas normas são genéricas e outras se aplicam a casos particulares. Nos próximos itens são descritos os principais objetivos de algumas das normas mais utilizadas no desenvolvimento de Sistemas Críticos.

2.6.1. Norma IEC 61508

Esta norma foi desenvolvida pelo IEC – *International Electrotechnical Commision* (IEC, 1997) e teve sua origem a partir de documentos feitos por dois grupos de estudo em 1991 e 1992. Em 1995 tais documentos foram reunidos e complementados, gerando a norma IEC 61508 – *Functional of Electrical/Electronic/ Programmable Electronic Safety–Related Systems*.

O escopo desta norma é o de prover guias de projeto voltados a sistemas eletrônicos e sistemas eletrônicos programáveis para Sistemas e Aplicações Críticas, sem se fixar em nenhuma aplicação particular.

Esta norma que possui 7 partes:

- Parte 1 - *General Requirements*: destaca o desenvolvimento de requisitos gerais de segurança, abrangendo conceito, escopo, definição e análise de risco e de perigo. Descreve ainda a alocação dos requisitos de segurança aos sistemas elétricos, eletrônicos e eletrônicos programáveis.

- Parte 2 - *Requirements for Electrical/Electronic/Programmable Electronic Systems*: nesta parte são refinados os requisitos desenvolvidos na parte 1, principalmente no que se refere ao projeto e fabricação de Sistemas Críticos.
- Parte 3 - *Software Requirements*: descreve a utilização de sistemas operacionais, software para redes de computadores, interfaces homem-máquina, ferramentas de suporte e linguagens de alto e de baixo nível. Estabelece também requisitos para o ciclo de desenvolvimento do software.
- Parte 4 - *Definitions and Abbreviations*: contém definições sobre todos os principais termos utilizados em todas as demais partes da norma.
- Parte 5 - *Examples of methods for the determination of safety integrity levels*: nesta parte da norma são detalhados exemplos de métodos a serem utilizados na determinação dos níveis de integridade de segurança, tais como a técnica ALARP já descrita, já descrita no item 2.1.3 desta tese.
- Parte 6 - *Guidelines for the application of parts 2 and 3*: fornece linhas mestras para a correta utilização das partes 2 e 3 da norma.
- Parte 7 - *Overview of Techniques and Measures*: descreve várias técnicas de desenvolvimento de software para Sistemas Críticos, como por exemplo, redes de Petri e métodos formais de especificação.

2.6.2. Norma RTCA – EUROCAE DO 178B

Esta norma - *Software Considerations in Airborne Systems and Equipment Certification* - foi elaborada conjuntamente por norte-americanos e europeus (RTCA, 1998), onde RTCA e EUROCAE significam respectivamente *Requirements and Technical Concepts for Aviation*. e *European Organization for Civil Aviation Electronics*. Esta norma é voltada para a aviação civil, constituindo-se em um acordo entre fabricantes europeus e norte-americanos da área da aviação. Sua edição inicial data de 1992, tendo recebido uma revisão em 1999.

O principal objetivo desta norma é o de prover guias para a determinação dos aspectos críticos de sistemas embarcados em aeronaves civis, não abrangendo a aviação militar.

A norma cobre apenas aspectos referentes ao software de sistemas embarcados, abrangendo seu ciclo de vida, o planejamento, o desenvolvimento, a verificação e a garantia da qualidade de software.

Na norma são definidos quatro níveis de segurança. O nível **D** é considerado o menos crítico, podendo ocasionar apenas desconforto à tripulação. O nível **C** representa problemas de segurança que causam desconforto aos passageiros e possíveis ferimentos. O nível **B** representa problemas perigosos, podendo ocasionar ferimentos fatais a um pequeno número de ocupantes da aeronave. Finalmente o nível **A** representa falhas catastróficas que afetam seriamente a segurança do vôo e de pouso da aeronave.

O FAA (*Federal Aviation Administration*), órgão regulador das atividades de aviação norte americanas, estabeleceu esta norma como o meio aceito para a certificação de todo novo software utilizado em sistemas aéreos (STOREY, 1996).

2.6.3. Norma HSE - *Health and Safety Executive*

HSE (*Health and Safety Executive*) é um órgão do governo britânico responsável pela regulação dos riscos à saúde e aos problemas relativos à Segurança Crítica oriundos de atividades em geral, tais como instalações nucleares, minas, indústrias, hospitais, prospecção de petróleo, transporte de mercadorias, dentre outras.

A norma *Guidelines Programmable Electronics Systems in Safety Related Applications* é uma das principais publicações do HSE, tendo sido editada em 1987, é composta por dois volumes. O primeiro é um guia introdutório sobre Segurança Crítica, para não especialistas nessa área. Esse primeiro volume descreve os aspectos básicos de sistemas eletrônicos programáveis, seus modos de falha e os métodos gerais de projeto de aplicações críticas (STOREY, 1996).

O segundo volume contém informações técnicas gerais, voltadas a engenheiros especializados. De forma mais detalhada, descreve a análise de perigo através de algumas técnicas e um estudo de caso de uma planta química de produção de explosivos.

O HSE possui centenas de outras publicações cobrindo, praticamente, todas as áreas que possam representar algum risco à saúde e à integridade das pessoas.

2.6.4. Normas da IAEA – *International Atomic Energy Agency*

A Agência Internacional de Energia Atômica é composta por 133 países membros, tendo 44 anos de existência. A IAEA estabelece diversas normas de segurança de instalações nucleares (IAEA, 2002a). Dentre elas há a norma IAEA *Safety Standard Series – Instrumentation and Control Systems Important to Safety in Nuclear Power Plants* – No.NS-6-13, de 2002 (IAEA, 2002b).

Essa norma provê auxílio no que se refere à Segurança Crítica no projeto de sistemas de controle e instrumentação de instalações nucleares. O uso de equipamentos de instrumentação e controle tem como objetivo controlar a reação nuclear, remover calor do reator e confinar a radioatividade. Esta norma descreve as funções de proteção, controle, monitoração e testes a serem realizadas em instalações nucleares. São descritos ainda os diversos tipos de equipamentos de instrumentação e controle no que se refere à proteção, intertravamento e redução de risco dessas instalações.

A norma contém ainda guias gerais de projetos referentes ao desempenho, confiabilidade, redundância, diversidade, independência, modos de falha, interface homem-máquina, qualidade, testes, manutenção e documentação dos equipamentos de instrumentação e controle. São também apresentadas as fases do ciclo de vida de desenvolvimento de sistemas de instrumentação e controle, bem como a verificação e validação desses equipamentos.

2.6.5. Norma NASA-STD-8719,13A

Esta norma - *Technical Standard – Software Safety* - descreve uma metodologia para a produção de software seguro a ser utilizado nos diversos programas comandados pela NASA – *National Aeronautics and Space Administration* (NASA, 1997).

A norma apresenta as atividades necessárias para se assegurar que um software adquirido ou desenvolvido pela NASA tenha o nível de Segurança Crítica adequado.

Também são descritas as atividades a serem executadas quando do ciclo de desenvolvimento de software para Sistemas Críticos, envolvendo as etapas de projeto, integração, implementação, operação, manutenção, controle e avaliação de alterações.

Em cada uma dessas etapas, a norma detalha quais são os requisitos gerais a serem aplicados, de forma a possibilitar a produção de programas que possam ser utilizados nos programas espaciais da NASA.

2.6.6. Norma EN 50126

Esta norma - RAMS - *Reliability, Availability, Maintainability, Safety* - é aplicável a sistemas de metrôs e ferrovias. É uma norma européia editada pelo CENELEC - *Comité Europeen de Normalisation Electrotechnique*, cuja última versão data de setembro de 1999 [CENELEC, 1999].

Esta norma é destinada às autoridades e indústrias ferroviárias, sendo aplicável em todas as fases do ciclo de vida de desenvolvimento de uma aplicação ferroviária, de modo a atingir os requisitos RAMS, ou seja, confiabilidade, disponibilidade, mantenabilidade e segurança crítica.

A norma define o conceito RAMS e o processo de desenvolvimento, baseando-se nas tarefas do ciclo de vida do sistema. Não são definidas quantidades ou soluções para aplicações ferroviárias específicas e não é contemplada a Segurança de Informação do sistema de supervisão e controle.

A norma é aplicável a qualquer ferrovia, seja em novos sistemas de controle e supervisão, seja em sistemas em modernização ou em expansão.

Os Conceitos de Segurança definidos na norma são baseados no conhecimento sobre todos perigos existentes no sistema, na severidade das conseqüências de cada perigo, nos modos de falha possíveis e na probabilidade de ocorrência de eventos.

2.6.7. Norma ENV 50129

Esta é uma norma européia editada pelo CENELEC - Co*mité Europeen de Normalisation Electrotechnique*, cuja última versão data de 1998 (CENELEC, 1998a).

Esta norma - *Safety Related Electronics Systems for Signalling* - aplica-se a sistemas eletrônicos de supervisão e controle que incluem hardware e software, sistemas esses utilizados em aplicações metro-ferroviárias. A norma abrange dois tópicos principais, que são o Gerenciamento da Qualidade e o Gerenciamento de Segurança.

O Gerenciamento da Qualidade descreve as atividades que visam minimizar a incidência de erros humanos, reduzindo o risco de falhas sistemáticas em módulos, sub-módulos ou equipamentos. Prevê ainda o controle de projeto, não-conformidade com especificações, ações corretivas, instalação e comissionamento, operação e manutenção, documentação, treinamento e auditorias.

O Gerenciamento de Segurança descreve as atividades a serem realizadas para a manutenção da segurança de sistemas, sub-sistemas ou equipamentos. A norma compara ainda o ciclo de segurança com relação ao ciclo de desenvolvimento. Outros aspectos contemplados pela norma são a organização das atividades de segurança, um plano de segurança, atividades afins e marcos principais.

Com este item encerra-se a descrição dos principais aspectos envolvidos na especificação, projeto e implementação de Sistemas Críticos. Resta a apresentação das principais Aplicações Críticas atualmente existentes, o que é feito no item a seguir.

2.7. Principais Aplicações Críticas

De forma a concluir este capítulo, neste item são descritas as principais áreas de Aplicações Críticas, destacando-se as principais características de cada uma delas.

2.7.1. Geração Nuclear de Energia

As usinas nucleares utilizam uma tecnologia potencialmente perigosa, visto que sua matéria básica é altamente radioativa e, praticamente, qualquer contato com esse tipo de material é fatal ao ser humano. Portanto, a indústria nuclear possui problemas de relacionamento com a população e com órgãos governamentais, e vem sempre buscando demonstrar que as usinas existentes ou a serem construídas não representam uma ameaça à comunidade.

Uma das formas de proteção em usinas nucleares é a utilização de proteção contra propagação ou falhas de funcionamento, incluindo o recipiente que contém o combustível nuclear, o sistema de refrigeração, escudos biológicos e o próprio edifício do reator. O projeto e a construção de usinas devem levar em conta todos os princípios de segurança, bem como o pessoal de operação e manutenção deve receber treinamento altamente especializado. Outra premissa de projeto utilizada é que a última medida de segurança, ou seja, aquela que seria a derradeira barreira contra um acidente, não deve depender de aspectos operacionais. São ainda previstas medidas de segurança secundárias projetadas para minorar conseqüências de eventuais acidentes.

Desta forma, a ocorrência de um acidente fica condicionada à ocorrência de distúrbios no processo nuclear, falhas no Sistema Crítico e das demais barreiras incluídas no projeto. Sempre visando a melhoria das condições de segurança em plantas nucleares, há propostas para que se automatizem suas tarefas mais rotineiras de monitoração, liberando os técnicos mais experientes para a execução de tarefas que exijam um acompanhamento mais cuidadoso (HUSSENINY et al., 1990). Esta é uma prática que pode se revelar salutar, visto que muitos acidentes em plantas nucleares ocorrem por falhas humanas em sua operação.

Em 1979, ocorreu um acidente na usina nuclear de *Three Mile Island*, localizada no estado da Pensilvania, nordeste dos Estados Unidos. Não houve nenhum efeito, sobre a saúde pública, decorrente do acidente e pouquíssima radioatividade foi liberada para fora da planta. A comissão que investigou o caso concluiu que uma série de eventos foi responsável pelo acidente, entre eles falhas de equipamentos (válvulas e bombas) e procedimentos operacionais inapropriados (LEVESON, 1995).

Outro acidente envolvendo usinas nucleares aconteceu na usina de Chernobyl, localizada na Ucrânia, antiga União Soviética. Em 1986, durante um teste que começou a ser realizado na usina, houve um incêndio e a liberação de material radioativo, causando a morte de 31 pessoas e a evacuação da população em um raio de 30 km da usina, sendo que o número total de mortes ou de casos de câncer atribuídos ao acidente é desconhecido. As causas desse acidente foram atribuídas a erros na operação da usina (LEVESON, 1995).

2.7.2. Processos Químicos

A necessidade de se tomar precauções relacionadas à segurança de Sistemas Críticos, na indústria química, fica evidenciada pela periculosidade dos materiais utilizados nos processos envolvidos. Os principais tipos de acidentes que podem ocorrer são incêndio, explosão e liberação de substâncias tóxicas (LEVESON, 1995).

Este último tipo de acidente, ou seja, a perda ou vazamento de substâncias é o mais grave na indústria química, justificando a preocupação maior quanto à sua prevenção, quando da análise de segurança em plantas químicas.

A existência de plantas químicas cada vez maiores, tendo como conseqüência o processamento e armazenamento de grandes volumes de materiais, com maior quantidade de energia contida nesses componentes são alguns fatores que justificam um aumento nas conseqüências produzidas por um acidente, tanto no que diz respeito a vidas humanas, quanto com relação ao ambiente. Outros dois fatores que contribuem para o agravamento dos acidentes são o pouco tempo disponível para acionar medidas de emergência e a proximidade cada vez maior das plantas químicas de aglomerações populacionais.

Um dos piores acidentes da história da indústria química ocorreu em 1984, em Bhopal, na Índia, na *Union Carbide*, onde ocorreu a liberação de metil-isocianeto (material utilizado na fabricação de pesticidas e de poliuretanos). Esta é uma substância perigosa tanto para seu armazenamento, quanto para seu manuseio, prejudicando a laringe, passagens nasais, olhos e pulmões. As causas do acidente foram a manutenção precária dos instrumentos de medição, principalmente de pressão e temperatura, e a não manutenção, na fábrica, de pessoal treinado e capacitado para a operação da planta. O número de mortes foi superior a 1.500 pessoas (LEVESON, 1995).

Na Inglaterra, a 250 km de Londres, ocorreu outro acidente significativo com a indústria química, envolvendo a indústria chamada Nypro. O acidente aconteceu em 1974, em virtude da instalação de uma tubulação provisória no processo de fabricação do caprolacto (utilizado na fabricação do nylon). Essa tubulação foi instalada, mas não foi devidamente projetada e testada, resultando em uma explosão que destruiu a indústria e os prédios em um raio de 500 m, matando 28 pessoas e ferindo outras 53 (LEVESON, 1995).

2.7.3. Aviação Comercial e Área Aeroespacial

O excelente nível de segurança obtido na aviação comercial e na área aeroespacial foi atingido graças a constantes pesquisas realizadas ao longo das últimas décadas. Para que esse nível de segurança seja mantido e até melhorado, faz-se necessária a aplicação de novos conceitos e técnicas, tendo em vista o crescente volume de tráfego aéreo verificado em todo o mundo.

Pode-se dizer que um dos fatores, que contribuiu em muito para que o bom nível de Segurança Crítica atual do transporte aeroviário fosse atingido e mantido, foi a análise cuidadosa de acidentes ocorridos, aliado a uma imediata realimentação dos dados colhidos, refletindo essas informações para o projeto e operação das aeronaves.

A preocupação inicial da indústria aeronáutica, no que se refere à Segurança Crítica, era a de que cada componente considerado isoladamente não apresentasse falhas. A

integridade de um elemento isolado mostrou-se adequada apenas para operações limitadas de vôo, mas não era apropriada para operações comerciais intensas.

No período de 1930 a 1945 ocorreu uma transição, objetivando-se a integração das partes, com a gradativa introdução de redundâncias e de projetos que procurassem evitar e tolerar a ocorrência de falhas.

O histórico mostra o sucesso das técnicas utilizadas, pois o número de acidentes aeroviários ocorridos em 1991 foi um quarto do número registrado em 1950, considerando-se ainda que o tráfego aéreo apresentou um aumento de aproximadamente 20 vezes nesse período (LILI, 1998).

Vale ressaltar que, atualmente, o controle do tráfego aéreo nas proximidades de um aeroporto está se tornando cada vez mais fundamental, principalmente se for observado que sua taxa de crescimento está estimada em torno de 70 % a cada 10 anos. Este aspecto é motivo de grande preocupação na área aeroviária (LILI, 1998).

Um acidente nessa área, que pode ser destacado, é o caso do avião DC-10, fabricado pela McDonnell-Douglas. Apesar de terem ocorrido diversos incidentes com o piso do compartimento de passageiros, ainda durante a fase de testes do avião, e de terem sido identificadas falhas no sistema de travamento do compartimento de bagagem, nada foi alterado no projeto, e o avião recebeu a certificação para vôo. No entanto, em 1974, um avião da *Turkish Air Lines* teve a porta do setor de carga aberta, causando o desabamento do piso do compartimento de passageiros e o rompimento de cabos de sinais de controle, ocasionando a perda de controle da aeronave. Houve 346 mortes (LEVESON, 1995).

Outro acidente na área aeroespacial foi o do ônibus espacial Challenger. A causa desse acidente, ocorrido em 1986, foi a falha de um anel de pressão na junta de um dos motores. Essa falha propiciou vazamento de combustível, que acabou por provocar uma explosão que destruiu a aeronave, alguns segundos após o seu lançamento. O problema começou com uma falha de projeto e se agravou à medida que a NASA (*National Aeronautic and Space Administration*) não reconheceu o sério problema existente, tratando-o inadequadamente (LEVESON, 1995).

2.7.4. Transporte Metro-Ferroviário

Os sistemas de transporte metro-ferroviários vêm sofrendo um processo de gradativa modernização, tendo em vista que apenas nas duas últimas décadas tem se verificado a substituição de antigos sistemas de supervisão e controle compostos por relés eletromecânicos, pela tecnologia de circuitos integrados, chegando até circuitos com processadores.

A separação de trens é um dos requisitos primordiais a serem seguidos quando do projeto de um Sistema Crítico voltado ao transporte metro-ferroviário. Em outras palavras, deve ser mantida uma distância segura entre dois trens consecutivos, de modo que a parada do trem que vai à frente, ainda possibilite a parada ou desvio do trem que vem atrás, sem causar uma colisão. Devem ser prevenidas rotas conflitantes, de modo que dois trens não devem ter o acesso liberado a um mesmo trecho de via, ao mesmo tempo, em sentidos inversos. Finalmente, o terceiro grande requisito de um sistema metro-ferroviário refere-se à monitoração da velocidade máxima permitida e ao acionamento automático de freios em caso de ultrapassagem de tal velocidade (The CHANNEL, 1994).

Recomenda-se que todos os subsistemas envolvidos em funções vitais do sistema de sinalização sejam projetados de forma que qualquer falha deve levar o sistema a uma condição segura.

Muitos acidentes metro-ferroviários têm ocorrido, e suas causas principais relacionam-se com problemas na sinalização e com procedimentos operacionais incorretos.

2.7.5. Equipamentos Médicos

A utilização de equipamentos cada vez mais sofisticados, na área médico-hospitalar, deve-se, em grande parte, ao avanço das técnicas da microeletrônica, possibilitando o desenvolvimento e fabricação de dispositivos cada vez mais precisos, compactos e eficientes. Com a utilização de computadores, puderam ser mais eficazmente controlados os diversos tipos de equipamentos médicos disponíveis, dentre eles aparelhos de raios X, de ultra-sonografia e tomografia, aparelhos para cirurgia a laser

e microcâmeras, bem como a geração de diagnósticos e o armazenamento dos dados mais significativos.

Os pacientes precisam ter plena confiança no funcionamento e no desempenho desses novos equipamentos, pois qualquer falha pode colocar em risco direto suas vidas, como por exemplo a radiação excessiva de um aparelho de raio X, ou um corte efetuado de forma incorreta por um aparelho de corte a laser (TSAI et al., 1997).

A interface com os usuários, em sua maioria não especialistas em computação, deve ser a mais amigável possível. É conveniente que tais interfaces possuam diversas verificações e confirmações a respeito de parâmetros fornecidos aos sistemas, de maneira a impedir a inserção de valores incorretos ou inseguros (TSAI et al., 1998).

A atuação de órgãos como o FDA (*Food and Drug Administration*) é de fundamental importância. O FDA fiscaliza e regulamenta, dentre outras, a indústria de equipamentos médicos norte americana, exigindo dos fabricantes a aplicação de técnicas e métodos apropriados que garantam o funcionamento correto de seus produtos (MOJDEHBAKHSH et al., 1994).

Um acidente notável ocorrido na nessa área é o caso do Therac 25, um equipamento de tratamento por radiação controlado por computador. Entre 1985 e 1987, 6 pessoas foram contaminadas por radiação excessiva originada do Therac 25. Dentre as causas desse acidente podem ser citadas falhas no software e a substituição de componentes mecânicos por computadores, sem a devida análise (LEVESON, 1995).

2.7.6. Indústria em Geral

As principais preocupações que surgem, quando se consideram as indústrias em geral, são ferimentos que possam ser causados a funcionários e danos às plantas industriais propriamente ditas. A realidade observada na maioria das indústrias é que as condições operacionais são bem conhecidas, sendo que até algumas condições perigosas acabam por ser aceitas. As técnicas de segurança que deveriam ser empregadas são, algumas vezes, consideradas ‘exageradas’ e de custo muito alto.

Desta forma, mesmo que tenham sido identificadas diversas condições adversas à segurança, elas são toleradas através de considerações do tipo: este é um evento de

ocorrência muito rara ou o custo para a eliminação desta condição perigosa não compensa as melhorias obtidas, e assim por diante.

Por exemplo, em indústrias com grande grau de automação, como a indústria automobilística, há uma grande utilização de robôs. Tais robôs devem ter seus movimentos programados com extrema precisão. Se houver algum tipo de problema com a movimentação desses robôs, podem ser atingidos operários que eventualmente estejam realizando atividades de monitoração.

Outra situação que pode ser citada é a que se observa na indústria siderúrgica, na qual o tamanho dos fornos e a quantidade de matéria prima envolvida tornam esse processamento extremamente crítico. Qualquer falha em seu Sistema Crítico pode provocar ferimentos ou mortes em muitos operários, ou mesmo sérios danos às instalações siderúrgicas.

Assim, neste capítulo foram descritos os aspectos mais relevantes referentes a Sistemas Críticos e à sua propriedade de Segurança Crítica. Para que seja possível realizar a comparação com os Sistemas de Informação e a Segurança de Informação, no capítulo a seguir são apresentados seus principais conceitos.

3. SISTEMAS DE INFORMAÇÃO

A informação, em suas diversas formas, tornou-se um bem universal, representando um fator de grande impacto em quase todas as atividades realizadas pelo ser humano.

Segundo um estudo realizado pela SIMS – *School of Information Management and Systems* da Universidade da Califórnia, Berkeley, no ano de 2001 a humanidade produziu o equivalente a 6 exabytes de informação, sendo que esse número vem dobrando a cada ano e inclui apenas uma versão original, não contabilizando réplicas (BERKELEY, 2002), (WINTER, 2002). A título de esclarecimento, 1 exabyte equivale a 1 milhão de terabytes ou a 10^{18} bytes.

Se for considerado que o espaço ocupado por um documento médio seja de 1 MB, isto significa que, em média, cada ser humano, seja homem, mulher ou criança, gerou 1000 documentos de 1 MB cada um, no ano de 2001, considerando-se uma população mundial de 6 bilhões de pessoas.

Toda essa informação deve ser organizada, pois de nada adiantaria tamanha quantidade, se ela não puder ser recuperada de forma simples e eficiente. A maneira mais comumente utilizada para a organização e disponibilização de tanta informação é através dos chamados Sistemas de Informação.

Um Sistema de Informação pode ser definido como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações para apoiar o processo de tomada de decisões e o controle de uma organização. Sistemas de Informação contêm informações sobre pessoas, lugares e coisas significativas dentro da organização ou do ambiente que a envolve (LAUDON; LAUDON, 2002).

A cultura de uma organização, o seu conjunto fundamental de suposições, valores e modos de realizar suas atividades podem ser embutidos em seu Sistema de Informação. Pode-se afirmar que Sistemas de Informação e organizações exercem influência mútua entre si. Por um lado os Sistemas de Informação devem estar alinhados com a organização, gerando as informações necessárias e importantes a

seus grupos. Por outro lado, a organização deve estar aberta às influências geradas pelo Sistema de Informação.

O domínio sobre todos os tipos de informação disponíveis é um fator de significativa importância no ambiente de negócios, cada vez mais competitivo que se observa nos dias atuais. Portanto, a informação deve receber toda a atenção possível, de forma a que sempre seja preservada sua consistência e sempre seja mantida a segurança das informações.

Toda a tecnologia disponível para o tratamento da informação deve estar inserida na política global da organização, que deve fornecer todo o apoio necessário, seja ele financeiro, logístico ou de pessoal, à implantação e manutenção dos Sistemas de Informação (KING, 2000).

A informação tem desempenhado um papel fundamental na política de condução dos negócios e atividades das organizações, sendo que essa importância será cada vez maior. Pode-se dizer que esse panorama vem ocorrendo em função do desenvolvimento de um relacionamento mais interativo com clientes, parceiros e fornecedores, compartilhando informações, bancos de dados, ferramentas, tecnologias e estratégias (LACITY, 2002).

Cada vez mais as aplicações estão sendo desenvolvidas para ambientes distribuídos e heterogêneos, principalmente para a Internet. As vantagens das aplicações distribuídas tornaram esse processo não uma opção, mas uma necessidade.

No entanto, esse processo tem levado as empresas a uma exposição maior, sujeitando-as a riscos relacionados com as possibilidades do uso indiscriminado de informações consideradas segredos de negócios.

Em aplicações distribuídas, nas quais o acesso pode ser feito por inúmeros usuários, há o problema de que se mantenha ou se procure manter a segurança das informações, visto que o vazamento de certos tipos de informação pode comprometer seriamente o bom andamento das atividades de uma organização.

Deve-se frisar que uma aplicação distribuída não é sinônimo de uma aplicação insegura. Basta que se utilizem os mecanismos apropriados para que o nível de Segurança de Informação seja mantido em patamares aceitáveis, tendo em vista que não é possível atingir uma segurança absoluta (DIAS, 2000).

Desta forma, nos próximos itens são descritas as principais técnicas utilizadas para a garantia da Segurança de Informação, as principais normas vigentes e algumas das principais aplicações dos Sistemas de Informação.

3.1. Segurança em Sistemas de Informação

A informação representa um patrimônio valioso para as organizações, justificando o emprego de todos esforços possíveis para garantir sua proteção e segurança, assegurando a continuidade dos negócios.

Sistemas de Informação estão inseridos em um ambiente computacional, e esse ambiente deve ser controlado e protegido contra desastres naturais (incêndios, terremotos), falhas estruturais (interrupções no fornecimento de energia), sabotagens, fraudes e acessos não autorizados.

A Segurança de Informação pode ser definida como a proteção de informações e de seu respectivo sistema computacional contra manipulações não autorizadas, falhas e desastres, de forma a reduzir a probabilidade de incidentes. Por incidente entende-se a perda de consistência dos dados, a sua alteração ou ainda o furto de informações por pessoas ou sistemas não autorizados.

Os objetivos básicos de uma política de Segurança de Informação são a redução da probabilidade de ocorrência de incidentes de segurança, a redução de danos causados por tais incidentes, bem como a recuperação em caso de problemas de segurança (MOREIRA, 2001).

Estatísticas mostram que 60% das empresas que vendem produtos ou serviços pela Internet acusaram, em um ano, um ou mais ataques a seus sites (PRICE, 2002). Esta estatística demonstra a gravidade do assunto, deixando claro que realmente há a necessidade de se prover mecanismos de proteção adequados e eficazes.

A abrangência da Segurança de Informação começa com a definição de uma política de segurança, passando pela análise de risco, pelos controles de acesso físico e lógico aos recursos computacionais, pelo treinamento e conscientização de funcionários, e finalizando com a existência de um plano de contingência.

Nos próximos itens são descritos os principais aspectos relacionados com a Segurança de Informação, principalmente no que se refere às ameaças e riscos a que Sistemas de Informação estão sujeitos.

3.1.1. Objetivos da Segurança de Informação

Os três objetivos básicos da Segurança de Informação são a manutenção da disponibilidade, da confidencialidade e da integridade da informação. Dito de outra forma, um usuário espera que as informações que ele procura estejam disponíveis no momento que ele necessitar, que estejam fora do alcance de pessoas ou sistemas não autorizados e que o conteúdo de tais informações não tenha sofrido qualquer problema de modificação indevida (DIAS, 2000).

A disponibilidade, conforme já definido, é a medida da probabilidade de um sistema estar sem falha em um determinado instante de tempo.

A confidencialidade visa proteger as informações contra o acesso por parte de pessoas ou programas não autorizados, mantendo o sigilo e a privacidade das informações.

Já a integridade das informações objetiva a proteção das mesmas contra qualquer tipo de alterações, sem que haja a autorização ou concordância do proprietário ou do responsável por tais informações.

A cada um desses três objetivos podem ser atribuídas prioridades, cujos pesos relativos dependem da natureza de cada aplicação, das ameaças e riscos a que se esteja sujeito e de prováveis impactos resultantes de violações da Segurança de Informação.

Duas das primeiras questões que se colocam, no tocante à Segurança de Informação, são que se determine as porções de informação que se deseja proteger e contra quem ou o que se deseja a proteção. Em seguida devem ser identificadas as ameaças mais prováveis e qual é o nível de proteção desejado. É indispensável que se saiba quanto tempo e recursos estão disponíveis para o desenvolvimento e implantação de políticas de Segurança de Informação, uma vez que devem ser contempladas no planejamento geral das empresas. Finalmente, é necessário que se conheçam quais são as expectativas de usuários e clientes em relação à Segurança de Informação e quais são as conseqüências para a organização em caso de violação das condições de segurança.

Desta forma, as linhas gerais da política de Segurança de Informação de uma organização é obtida a partir da resposta a esses aspectos. As medidas preventivas devem ser definidas de forma a atender aos requisitos da política de segurança, levando em consideração o equilíbrio entre os fatores custo da implementação de medidas de segurança e os respectivos benefícios associados.

Para que uma política de Segurança de Informação tenha sucesso, é indispensável que haja o comprometimento da alta direção das empresas, não apenas no que se refere à liberação de recursos, mas também na questão de se fazer da Segurança de Informação uma prioridade dentro da organização.

Outro fator a ser considerado é que as medidas da Segurança de Informação devem ser tratadas e planejadas a priori, nas fases iniciais do desenvolvimento do sistema, e não após sua entrega ou depois da ocorrência de um incidente relacionado à Segurança de Informação.

A política de Segurança de Informação adotada deve ser adaptável, permitindo a realização de alterações, sempre que estas se fizerem necessárias, em decorrência de alterações no ambiente em que estiver inserido o Sistema de Informação. Essa política de segurança deve ter ampla divulgação na organização, inserindo-se em sua política global e, deve sempre estar de acordo com as leis vigentes no país.

Além disso, as responsabilidades de todos os membros da organização devem ser claramente definidas.

3.1.2. Mecanismos de Segurança de Informação

A implementação de mecanismos de Segurança de Informação deve começar desde o controle físico do ambiente computacional, passando pelo controle lógico, através de autenticações e controle de acesso, indo até o controle humano, representado pelo treinamento de funcionários e realizações de auditorias.

Dentre os principais recursos e informações a serem protegidos estão programas aplicativos, arquivos de dados, utilitários, sistema operacional, arquivos de senha e arquivos de histórico de uso (DIAS, 2000).

A proteção de programas aplicativos, sejam programas fonte ou programas executáveis, visa impedir sua alteração ou ainda sua execução indevida. Arquivos de dados devem ser protegidos para evitar consultas e alterações indevidas a dados vitais ao negócio da organização.

Um dos objetivos da proteção ao uso de programas utilitários é evitar o emprego de editores e compiladores do próprio sistema, pois podem ser utilizados para alterar programas e dados.

O sistema operacional se constitui em um ponto chave do controle do esquema de segurança, visto que uma possível fragilidade no mesmo, representa a porta de entrada a qualquer sistema computacional.

O acesso aos arquivos de senha permitiria o conhecimento do conteúdo de arquivos com as senhas do sistema, o que representaria a possibilidade de acesso livre e irrestrito aos recursos do sistema.

Finalmente, bloquear o acesso aos arquivos de histórico de utilização objetiva impedir que ações ou operações irregulares possam ser encobertas, pela alteração desses arquivos.

Alguns dos principais mecanismos adotados para se proteger de riscos e, portanto preservar a segurança de um Sistema de Informação são o uso de criptografia na transmissão de mensagens, certificação digital para acesso a informações, segurança física, existência de um plano de contingência, detecção de invasões, realização de

auditorias e existência de programas antivírus (DIAS, 2000). Alguns desses mecanismos são descritos nos próximos itens.

3.1.2.1. Controles de Acesso Físico

O propósito dos controles de acesso físico é o de impedir que pessoas não autorizadas obtenham acesso físico a certos objetos. Em geral a segurança física é obtida escondendo-se ou ocultando-se a localização dos objetos, ou ainda isolando-os e protegendo-os, dificultando ainda mais o acesso aos mesmos. Por objetos entendem-se os equipamentos que compõem o sistema computacional que aloja o Sistema de Informação.

Os controles de acesso físico têm como finalidade permitir que apenas as pessoas autorizadas tenham acesso ao ambiente físico que contém os recursos computacionais da organização.

Podem ser definidos três ambientes no que se refere à segurança física de um ambiente computacional (HUNTER, 2001):

- Ambiente Global de Segurança: área sobre a qual a organização mantém alguma forma de controle ou influência, tal como estacionamentos ou áreas vizinhas à instalação computacional;
- Ambiente Local de Segurança: salas adjacentes ao local da instalação computacional. O controle de quais pessoas entram ou saem deste ambiente deve ser feito de acordo com as medidas necessárias pré-estabelecidas. Dentro deste ambiente local, pode haver diferentes regiões com controles de acesso distintos.
- Ambiente Eletrônico de Segurança: sala onde se localiza efetivamente a instalação computacional e todos seus equipamentos periféricos. Os recursos a serem protegidos e que se encontram no ambiente eletrônico de segurança são servidores, impressoras, terminais, roteadores, scanners, etc.

O acesso aos ambientes pode ser feito por intermédio de controles explícitos e de controles de regulamentação de acesso. Os controles explícitos são representados por fechaduras mecânicas e eletrônicas, câmeras de vídeo, alarmes e guardas de

segurança. Os controles de regulamentação ao acesso são constituídos por senhas, cartões ou sistemas de identificação biométricos.

O acesso, por pessoas supostamente conhecidas, tais como visitantes, clientes e outros não diretamente envolvidos com a operação do sistema computacional, deve ser feito sob certas restrições. O contato dessas pessoas com o sistema computacional deve ser o menor possível.

3.1.2.2. Controles de Acesso Lógico

Considerando-se que controles de acesso físico não são suficientes para garantir a segurança de informações de um sistema computacional, são necessários controles de acesso lógico, representados por medidas de segurança implementadas por hardware e por software para impedir acessos não autorizados ao sistema.

O principal objetivo do controle de acesso lógico é o de que apenas usuários autorizados tenham acesso aos recursos computacionais e que esse acesso seja apenas aos recursos realmente necessários à execução de suas tarefas. Isto significa que, usuários devem ser impedidos de executar transações incompatíveis com suas funções ou além de suas responsabilidades.

Na tentativa de acesso ao sistema, entram em ação os controles de acesso lógico, envolvendo o fornecimento da identificação do usuário e de uma senha que serve de autenticação, provando ao sistema que o usuário é realmente quem diz ser. O identificador de cada usuário deve ser único, ou seja, cada usuário deve ter sua identidade própria. Como autenticação podem ser usadas senhas, cartões inteligentes, características físicas como impressão digital, voz ou retina (características biométricas de uma pessoa).

A identificação baseada em uma característica física do usuário (identificação biométrica) visa suprir deficiências de segurança de senhas que podem ser reveladas ou descobertas e de objetos, como cartões magnéticos ou cartões inteligentes, que podem ser perdidos, roubados ou reproduzidos.

3.1.2.3. Segurança na Comunicação

Atualmente não se concebe um sistema computacional completamente isolado dos demais, havendo a necessidade de comunicação com outros sistemas computacionais. É justamente na comunicação que surgem os principais problemas de segurança em Sistemas de Informação.

Usuários não autorizados podem se conectar e passar por usuários autorizados. Se um invasor conseguir se fazer passar como um usuário legítimo, provavelmente terá o acesso facilitado a todas as informações que desejar furtar ou adulterar. Mesmo usuários autorizados têm restrições de acesso. Eles podem tentar burlar os controles e executar operações ou obter dados a que não teriam direito.

No sentido de procurar estabelecer algumas normas mínimas de segurança, o governo britânico estabeleceu uma diretriz para conter ou minimizar ataques a sistemas computacionais (HUNTER, 2001). Se qualquer parte de um sistema ou rede de computadores transportar informações sigilosas sobre o andamento de projetos e negócios de uma empresa, e for acessível por áreas não controladas (por ex. rede pública de telefonia), a comunicação deve ser protegida por métodos de criptografia.

Uma das formas de se aperfeiçoar a segurança na comunicação e no armazenamento de dados é através da criptografia. A criptografia compreende a codificação, pelo sistema que estiver gerando mensagens ou dados, e a decodificação, pelo sistema destinatário das mensagens ou dados. Os dois principais mecanismos de criptografia são chamados de simétrico e assimétrico.

No mecanismo simétrico, tanto o transmissor de mensagens ou dados, quanto o receptor, utilizam uma mesma chave secreta para codificação e decodificação. No mecanismo assimétrico, a chave de codificação do transmissor de mensagens ou dados é diferente da chave de decodificação do receptor.

Outra forma de se aprimorar a segurança na comunicação de dados é por meio do estabelecimento de diálogos de autenticação e de *firewalls*.

Se um invasor se apossar da identidade de um usuário legítimo, através de monitoração do diálogo desse usuário com o sistema, pode acessá-lo de maneira mais fácil. Daí surge a técnica dos diálogos de autenticação, cuja seqüência depende do instante de comunicação e do seqüenciamento de mensagens trocadas.

Os *firewalls* se constituem em equipamentos com o propósito de bloquear pacotes de protocolos não autorizados (atuando como filtro de pacotes), bem como ocultar, de invasores, a estrutura interna de um site.

Pode-se citar algumas outras formas de proteção, tais como a assinatura digital, o preenchimento de tráfego e o controle de roteamento. A técnica de assinatura digital consiste na emissão de uma assinatura digital e na verificação dessa assinatura. O preenchimento de tráfego compreende a geração de mensagens aleatórias, sem nenhuma informação útil, apenas com a finalidade de enganar observadores não autorizados. Por sua vez, o controle de roteamento visa prevenir tráfego de dados críticos em canais de comunicação mais vulneráveis.

Neste item foram descritas algumas maneiras de se tentar impedir que um invasor consiga acesso ao Sistema de Informação. Caso não se obtenha sucesso através das medidas descritas, faz-se necessária a elaboração de um plano de contingência e de recuperação de desastres, descrito a seguir.

3.1.3. Plano de Contingência e Recuperação de Desastres

Não há medidas de proteção com eficácia total, ou seja, que de fato consigam impedir completamente a ocorrência de invasões e de incidentes em um Sistema de Informação. Tendo em vista tal situação, é necessário que, além de tais medidas de proteção, exista um plano de contingência e um plano de recuperação de desastres.

O plano de contingência visa manter a operação do Sistema de Informação, mesmo na ocorrência de qualquer problema que possa ter ocorrido, seja uma invasão com adulteração de dados, seja um acidente natural, como um incêndio no sistema computacional.

Caso ocorra algum evento que impossibilite o funcionamento total do Sistema de Informação, este deve continuar a operar, dependendo da extensão do problema, com um certo grau de degradação,.

Após esta fase inicial, de manutenção ou colocação do Sistema de Informação em funcionamento, seja pleno, seja com alguma espécie de degradação de suas funções, vem a fase de recuperação do desastre. Esta fase consiste na substituição dos recursos computacionais, provavelmente afetados, por outros recursos previamente alocados para essa função, possibilitando um funcionamento normal e com todas as funções originais do sistema.

Os planos de contingência e de recuperação de desastres não aumentam, diretamente, a lucratividade da instituição, mas evitam maiores perdas em decorrência de incidentes que possam vir a ocorrer.

Quanto mais tempo um Sistema de Informação não estiver disponível, maiores serão os impactos nos negócios de uma organização. Uma das metas de um plano de contingência é minimizar o tempo de parada dos sistemas, visando a redução dos impactos nos negócios e a proteção das informações institucionais.

A disponibilidade de serviços de informação e a confiabilidade em seus dados influem diretamente na credibilidade da instituição.

3.1.3.1. Fases do Plano de Contingência

As fases que compõem um plano de contingência são a realização de análises preliminares, a análise de impacto, a análise das alternativas de recuperação, o desenvolvimento do plano de contingência propriamente dito, o treinamento e testes do sistema e a avaliação dos resultados e possíveis atualizações do plano (MAIWALD; SIEGLEIM, 2002).

Na fase de Análises Preliminares, uma das tarefas é a de procurar envolver e conscientizar a alta direção da empresa sobre a importância da implementação de um plano de contingência, que sempre envolve a aplicação de recursos financeiros. Também são importantes as tarefas de conscientização de funcionários, a definição

de prazos e a realização de um estudo preliminar envolvendo a identificação das funções e recursos críticos ao Sistema de Informação.

Na fase de Análise de Impacto é feita a identificação de impactos sobre a instituição, ou seja, dos danos potenciais que uma ameaça possa causar, ao ser concretizada. Deve ser feita uma avaliação do tempo que cada atividade, sistema ou recurso pode ficar indisponível ou com funcionalidade reduzida.

Na fase da Análise das Alternativas de Recuperação, realiza-se um estudo sobre as alternativas existentes, visando a recuperação dos serviços computacionais. A manutenção de cópias de segurança, juntamente com procedimentos e infraestrutura necessária à proteção e à recuperação das informações é uma das alternativas possíveis. Outra possibilidade é a manutenção do chamado *hot site*, que se constitui em um local alternativo de processamento paralelo que, em caso de qualquer problema no site principal, está pronto para assumir imediatamente o comando do sistema. Esta última possibilidade é bastante eficiente, porém apresenta alto custo de implementação.

Na fase de Desenvolvimento do Plano de Contingência, efetua-se o seu detalhamento e identificam-se os recursos necessários. Os principais passos a serem executados em resposta a um desastre são: identificação e compreensão do problema, contenção dos danos, limitando ou resolvendo o problema, determinação dos danos causados, restauração dos sistemas à sua operação normal e eliminação das causas, para que o problema não ocorra novamente. Deve ser designado um grupo de recuperação de contingências, que envolve desde um representante da gerência, até o pessoal estritamente técnico.

Para que o Plano de Contingência possa funcionar, faz-se necessário fornecer o treinamento e a conscientização adequados a todos os responsáveis pelo plano, na organização.

É vital que o plano seja testado, de forma a se poder verificar se todos os pontos estão sendo cobertos de forma adequada. Os testes podem envolver o próprio sistema, ficando bem próximos da realidade, realizados de forma integral ou parcial, ou podem ainda ser simulados, através de representações das situações de emergência.

Finalmente o Plano de Contingência deve ter seus resultados avaliados e, se necessário, sofrer as devidas atualizações.

3.1.3.2. Fases da Recuperação de Desastres

A recuperação de desastres visa manter a disponibilidade de um Sistema de Informação. Por recuperação entende-se a habilidade de uma empresa em se recuperar de um incidente de segurança, ou seja, a empresa deve estar apta a continuar operando seus Sistemas de Informação, não importa o tipo de incidente que ocorra. O nível de recuperação é determinado pelos tipos de incidentes que possam afetar a empresa e pelos impactos potenciais de um incidente de Segurança de Informação (MASSIGLIA; MARCUS, 2002).

Normalmente ocorrem conflitos entre a eficiência de um negócio, que pode ser entendida como fazer o que deve ser feito, utilizando o mínimo possível de recursos, e a recuperação, que significa fazer o que deve ser feito sem interrupção significativa de funcionamento (BYRNES; KUTNICK, 2002).

O plano de recuperação de desastres implementado em uma empresa deve prever a possibilidade da execução de cada função em, no mínimo, dois locais. Mais ainda, sempre deve haver mais de um funcionário capacitado a realizar cada tarefa. Dessa forma, os custos operacionais têm um acréscimo, às vezes significativo, em decorrência da implantação de um plano de recuperação.

É necessário analisar a empresa para se verificar quais são os principais pontos a serem preservados, pois nem sempre é possível proteger toda a organização contra um incidente.

Um plano de recuperação é um conjunto de ações que deve ser capaz de responder a duas questões básicas. A primeira delas é, se um incidente ocorrer, fazendo com que

uma determinada função fique inoperante, como tal função será restaurada. A segunda questão que se coloca é, se durante a recuperação de um incidente, outro incidente ocorrer, levando uma segunda função a se tornar inoperante, como serão resolvidos eventuais conflitos de demanda requeridos para recobrar as duas funções afetadas.

Portanto, no plano de recuperação, é importante que se identifiquem as prioridades de cada aspecto do funcionamento do sistema, bem como as formas de resolução de conflitos, possivelmente existentes, para que a recuperação seja viável.

É importante que um plano de recuperação seja escrito de maneira clara e sucinta, que seja divulgado a todos funcionários da organização e que seja atualizado periodicamente, refletindo alterações nas condições da empresa, bem como de novas ameaças.

Até aqui foram descritas as principais atividades técnicas necessárias à manutenção da Segurança de Informação em Sistemas de Informação. Nos próximos itens são descritos dois aspectos de extrema importância no que se refere à manutenção da segurança em Sistemas de Informação, que são a cultura de segurança e os requisitos de segurança aplicáveis a esses sistemas.

3.2. Cultura de Segurança em Sistemas de Informação

Assim como no caso da Segurança Crítica, pode-se dizer que não há uma técnica absoluta que garanta, pela sua simples aplicação, a solução de todos os problemas de Segurança de Informação.

É necessária a existência de um programa de conscientização que prepare as pessoas para entenderem, aceitarem e participarem do processo de implementação da Segurança de Informação.

O treinamento, no que se refere à Segurança de Informação, deve ser constante, de tal forma a manter todo o corpo de funcionários atualizado quanto aos conceitos e

normas implementados, bem como obter a consciência e o comprometimento de todos com o processo de garantia da Segurança de Informação.

Parte do processo de implementação de Segurança da Informação pode ser automatizado ou controlado através de ferramentas especificamente adquiridas para tal finalidade. Porém, a equipe encarregada do projeto da Segurança de Informação deve ser capacitada, de forma a transmitir confiança e credibilidade, antes, durante e após o processo de implementação de garantia da Segurança de Informação.

É de fundamental importância que seja estabelecido e claramente divulgado, a toda organização, um conjunto de normas e diretrizes, as quais devem descrever os objetos a serem protegidos, contra o quem e contra o que proteger, além das principais medidas a serem acionadas em caso de incidentes de segurança.

A tecnologia empregada auxilia e é até fundamental para a implantação de um programa de Segurança de Informação, mas deve sempre ser acompanhada da conscientização de funcionários, da direção da empresa e também de seus clientes.

Os principais fatores de risco que se apresentam em um Sistema de Informação são constituídos pelos funcionários da própria organização detentora do sistema, por invasores externos e pelo ambiente do sistema computacional.

Os próprios funcionários podem cometer erros, utilizar indevidamente os sistemas ou mesmo realizar atos de sabotagem. Invasores externos provavelmente se constituem no tipo de ameaça mais temido, podendo ocasionar todos os tipos de problemas já citados, tais como roubo de informações, destruição ou alteração deliberada de informações ou ainda inclusão de informações com o intuito de sabotar ou confundir usuários autorizados do sistema. No que se refere ao ambiente do sistema computacional, há o risco de interferências eletromagnéticas, bem como de desastres naturais, tal como um incêndio.

O gerenciamento desses riscos tem como objetivo limitar os efeitos de ataques a um Sistema de Informação, possuindo dois tipos de controle, o preventivo e o corretivo. Os controles do tipo preventivo têm como função evitar a ocorrência de problemas de Segurança de Informação. Já os controles do tipo corretivo têm por função controlar os impactos decorrentes da quebra dessa segurança.

A implementação das práticas de segurança não se resume aos meios técnicos, mas também a práticas administrativas, que incentivem funcionários e clientes a colaborarem ativamente no processo.

As práticas de Segurança de Informação são resultado de experiências adquiridas em processos de garantia da segurança. Por outro lado, práticas de segurança não são simples mecanismos da Tecnologia da Informação implementados através de hardware e de software. Para a garantia da Segurança de Informação, não necessariamente deve ser empregada a mais moderna e melhor prática desenvolvida, mas sim a prática mais factível. Atos isolados não são suficientes para garantir a Segurança de Informação, mas sim um conjunto de diretrizes e procedimentos.

Nem sempre a técnica mais refinada ou teoricamente mais perfeita em termos de proteção é, necessariamente, a mais adequada a qualquer situação. Eventualmente, cada tipo de atividade deve passar por um processo de aprendizado e prática, de forma a identificar as melhores técnicas e ferramentas a serem utilizadas para a garantia da Segurança de Informação.

Não devem ser abertas lacunas em nenhuma ocasião, ou seja, a preocupação com a Segurança de Informação deve ser uma constante durante todo o tempo, para todos os funcionários, desde o mais simples técnico, até o presidente da organização.

A difusão do conhecimento nessa área da Segurança de Informação também se enquadra na área da Gerência do Conhecimento. Às vezes não se consegue exprimir o conhecimento tácito, possuído por pessoas, em um documento, sendo necessário um contato pessoal para a sua transmissão a outras pessoas.

Assim como em outras áreas, o desenvolvimento de práticas adequadas de Segurança de Informação também tem um ciclo, composto pela identificação e a avaliação das melhores práticas de acordo com determinados critérios, a adoção e a documentação das práticas selecionadas e eventuais adaptações ou melhorias que se façam necessárias, em virtude de constantes inovações tecnológicas e a alterações do ambiente.

Um dos aspectos de maior relevância dentro de uma cultura de Segurança de Informação se constitui na definição dos requisitos de segurança aplicáveis a tais sistemas, o que é descrito a seguir.

3.3. Requisitos de Segurança de Informação

O objetivo inicial dos primeiros Sistemas de Informação, no que se refere à sua segurança, restringia-se ao controle de acesso físico aos locais onde se situavam os sistemas computacionais. No entanto, ocorreu uma grande mudança nesse conjunto original de requisitos, passando a incluir a identificação e autenticação para o acesso lógico aos recursos dos sistemas. Tais recursos, a cada dia que passa, tornam-se mais valiosos, principalmente no que se refere aos dados neles armazenados.

Outra área incluída nos requisitos de Segurança de Informação e de extrema importância, é a da comunicação entre computadores, que se constitui na principal porta de entrada de intrusos aos Sistemas de Informação.

Os requisitos de um Sistema de Informação devem incluir a proteção contra todos os riscos identificados, incluindo-se riscos internos e externos.

Pode-se dizer que os ataques terroristas ocorridos nos últimos anos também foram um fator propulsor dessa maior preocupação com a Segurança de Informação, visto que há diversos sistemas, muitos deles governamentais, que despertam grande cobiça por pessoas ligadas a esses grupos terroristas (GHOSH, 2002).

Pode-se dizer que a maior fonte de resistência à utilização do comércio eletrônico seja a falta de confiança e o receio de existência de pontos vulneráveis na Segurança de Informação e na infraestrutura utilizada para tais sistemas. Tais pontos falhos podem resultar em acessos não autorizados a recursos, enxerto de vírus de computador, roubo de dados e até mesmo destruição da partes da infraestrutura computacional.

Um ataque a uma rede de computadores pode afetar a milhares ou mesmo milhões de pessoas, como por exemplo, a invasão de computadores de bolsas de valores, de instituições financeiras, de monitoramento de pacientes em um hospital, de vendas de passagens, etc.

Alguns sistemas, buscando uma maior segurança a seu acesso, já incluem em seus requisitos de segurança a necessidade do uso da identificação através de características físicas de seus usuários, tais como a impressão digital, a voz ou a íris, dentre outros (no item 5.1.1 há mais detalhes sobre as formas de identificação biométricas).

Outro ponto bastante importante é a especificação da utilização de técnicas de criptografia de dados. Praticamente não se concebe mais a existência de comunicação de dados de valor sem a utilização da criptografia para a sua proteção.

Quando do projeto da segurança para um Sistema de Informação, deve-se realizar um estudo detalhado, visando verificar se os investimentos estão sendo dirigidos para as áreas que apresentem os maiores riscos de invasões.

Conforme já descrito, os três principais aspectos a serem tratados em Sistemas de Informação, no que se refere à Segurança de Informação, são a disponibilidade, a confidencialidade e a integridade dos dados, e por conseguinte, todos devem ter seus requisitos especificados.

Há uma série de aspectos comuns a todos os Sistemas de Informação, que devem ser especificados, como a existência de um plano de contingência, de um plano de recuperação de desastres e da minimização de conseqüências em virtude de um problema de segurança.

Outro grupo de fatores que sempre deve estar presente nos requisitos é a especificação das manutenções preventiva e corretiva. Com respeito à manutenção preventiva, devem ser estabelecidos intervalos mínimos necessários à realização desse tipo de manutenção, visando manter a disponibilidade desejada. Já com relação às manutenções corretivas, devem ser estabelecidos tempos máximos para que a equipe de manutenção consiga reparar todos os módulos que possivelmente tenham apresentado problemas, restaurando a condição inicial do sistema.

Requisitos não diretamente ligados à Segurança de Informação também devem ser especificados, como, por exemplo, o desempenho e a capacidade de armazenamento de dados.

Após terem sido analisados os principais requisitos aplicáveis a Sistemas de Informação, faz-se necessária uma descrição das principais formas de implementação encontradas para tais sistemas, bem como as principais formas de armazenamento lógico dos dados disponíveis, o que é feito no item a seguir.

3.4. Implementação de Sistemas de Informação

A implementação dos Sistemas de Informação e de suas medidas de Segurança de Informação representa um fator de grande importância, tendo em vista a função vital que tais sistemas desempenham. Sendo assim, neste item são descritas as principais formas de implementação de Sistemas de Informação no que se refere ao seu hardware e ao seu software, representado pelas tecnologias de armazenamento e recuperação de dados.

3.4.1. Arquitetura de Sistemas de Informação

O principal tipo de arquitetura utilizada em Sistemas de Informação é a Arquitetura Cliente/Servidor. Um cliente é definido como um solicitador de serviços e um servidor como um provedor desses serviços. Esta arquitetura veio em substituição aos *mainframes*, nos quais todo o processamento é feito em um computador central. Uma tendência que vem se observando, ultimamente, é a de utilização dos *mainframes* como servidores, em uma arquitetura cliente/servidor (BRITTON, 2001).

As primeiras redes de computadores pessoais baseavam-se em uma arquitetura de compartilhamento de arquivos, na qual um servidor repassava arquivos aos computadores pessoais, que eram então encarregados de executar o processamento desses arquivos. Este tipo de arquitetura apresenta bom funcionamento apenas com um pequeno número de computadores conectados a um servidor, em virtude do tráfego pela rede.

A arquitetura cliente/servidor veio em resposta a essa limitação, sendo o servidor de arquivos substituído pelo Servidor de Dados, caso em que apenas a resposta é transmitida ao cliente, e não um arquivo de dados completo.

As principais características observadas na Arquitetura Cliente/Servidor são (BRITTON, 2001):

- Clientes e servidores são módulos funcionais com interfaces bem definidas (não é necessário o acesso a suas estruturas internas);
- A relação cliente/servidor é estabelecida entre dois módulos funcionais, quando um módulo (cliente) requisita um serviço e outro módulo (servidor) responde à requisição;
- A troca de informações entre cliente e servidor ocorre apenas através de mensagens (não há variáveis globais). Tanto a requisição de serviço e informações adicionais, quanto a resposta do servidor são colocadas em mensagens;
- Clientes e servidores estão, normalmente, em máquinas separadas, conectados por uma rede.

Os principais tipos de implementação dessa arquitetura são a de duas camadas (*two-tier*), três camadas (*threee tier*) e n-camadas.

3.4.1.1. Camadas da Arquitetura Cliente/Servidor

O primeiro tipo de arquitetura cliente/servidor utilizado foi a arquitetura com duas camadas. Nesse caso, a aplicação é dividida em duas camadas lógicas. A primeira camada, que são os clientes, representa o *front-end*, ou seja, contém a interface gráfica do usuário e a lógica de negócio da aplicação. A segunda camada é composta pelo Servidor, representando o *back-end* das aplicações. A figura 3.1 apresenta esquematicamente essa arquitetura.

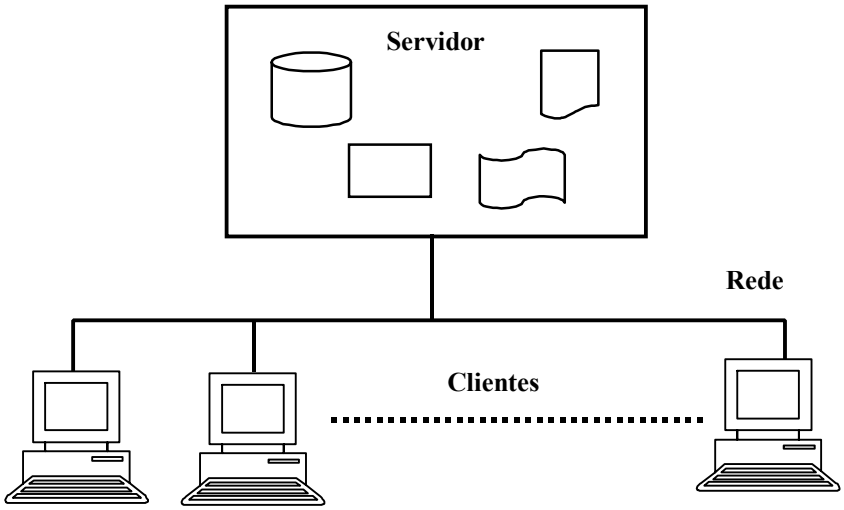

Figura 3.1 – Arquitetura de Duas Camadas

Normalmente, cada camada é executada em máquinas distintas. O Servidor realiza o acesso direto a todos os serviços disponíveis, tais como bases de dados, impressoras e gerenciador de tarefas, dentre outros.

O segundo tipo de arquitetura cliente/servidor utilizado é a arquitetura de três camadas. Neste caso a aplicação é dividida em três camadas, conforme apresentado na figura 3.2.

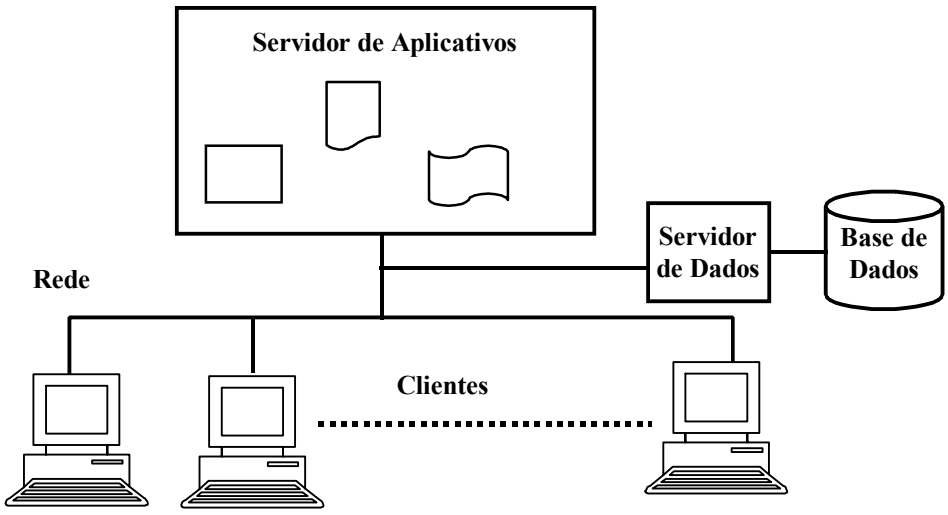

Figura 3.2 – Arquitetura de Três Camadas

O processamento da lógica de negócios vai para o Servidor de Aplicativos. Para acrescentar novos clientes basta instalar outros Servidores de Aplicativos ou aumentar a capacidade de processamento dos Servidores já existentes. Alterações nas

regras de negócio são feitas apenas nos Servidores de Aplicativos e não em todos os clientes. A principal alteração está na separação do Servidor de Dados, responsável pelo acesso às Bases de Dados do sistema.

Algumas vezes, o Servidor de Aplicativos é dividido em duas ou mais unidades com diferentes funções, sendo que tal arquitetura é então chamada de multicamadas. Este é o caso em algumas aplicações Internet, que têm clientes magros, escritos em HTML (*Hyper Text Markup* Language) e servidores de aplicações escritos em C++ ou Java. A distância entre esses tipos de aplicações é muito grande, levando à colocação de uma nova camada entre o Servidor de Aplicativos e os Clientes, representada pelo Servidor Web. A figura 3.3 apresenta esquematicamente essa arquitetura.

Finalmente, há a arquitetura de N camadas, representada na figura 3.4. Esta arquitetura pode ser implementada por meio do padrão CORBA – Common Object Request Broker, padronizada pelo OMG – Object Management Group. O objetivo desta padronização é procurar solucionar os problemas de interoperabilidade existentes em sistemas distribuídos, pela utilização da técnica de orientação a objetos. Nesta arquitetura, clientes e servidores são conectados por um middleware conhecido como ORB – *Object Request Broker*, que realiza a comunicação entre os diversos objetos existentes no sistema.

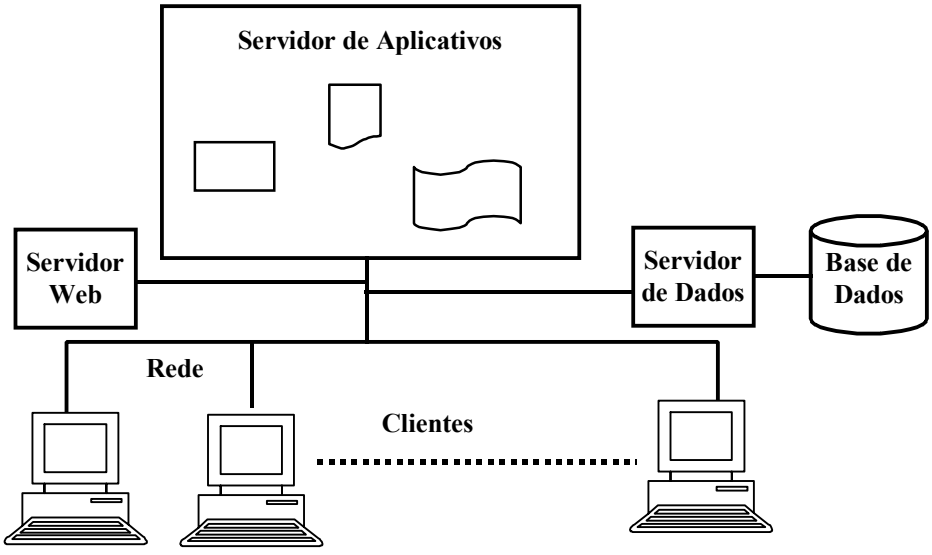

Figura 3.3 – Arquitetura de Quatro Camadas

Objetos enviam requisições de serviços, que são recebidas pelo *middleware* ORB. Esta por sua vez, localiza os objetos necessários, representados pelos servidores, efetuando sua ativação.

Este tipo de arquitetura é conhecido como N Camadas, pelo fato de que podem existir tantos Servidores, quantos sejam necessários. A denominação mais conhecida para este tipo de arquitetura é Arquitetura de Objetos Distribuídos.

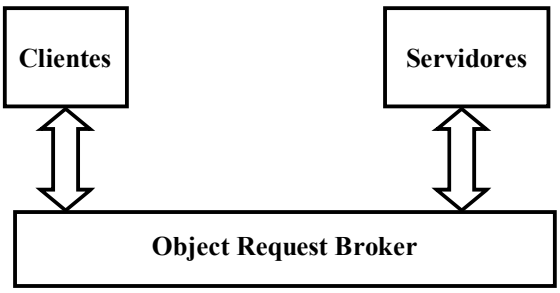

Figura 3.4 – Arquitetura de N Camadas

3.4.1.2. Clustering

Em um Sistema de Informação busca-se um alto índice de disponibilidade. A alta disponibilidade é obtida, na maioria das vezes, por meio da aplicação de técnicas de tolerância a falhas. Isto é feito através da redundância de módulos, identificando-se aqueles mais propensos a falhar e instalando componentes redundantes a tais tipos de dispositivos. Este é o princípio da técnica de *cluster*.

Cluster é um tipo de arquitetura que consiste em um conjunto de um ou mais computadores interconectados, chamados de nós, que podem ser encarados como um único recurso computacional, visando a melhoria de disponibilidade e de desempenho. Através desta técnica, torna-se possível garantir serviços com tempos de interrupção reduzidos.

A principal dificuldade encontrada na *clusterização* está no gerenciamento do funcionamento de diversas máquinas, de forma coordenada.

Há aplicações que não podem tolerar tempo significativo fora de operação, nem a perda de dados ou ainda a existência de pontos críticos de processamento. A técnica de *clusterização* pode colaborar em muito para uma melhora da disponibilidade, confiabilidade e balanceamento da carga de processamento desses sistemas.

A utilização de *clusters* provê mecanismos para tratar falhas de hardware e de software, mantendo uma imagem das atividades do servidor em um sistema secundário ou de *backup*. Quando uma falha é detectada no nó primário, o nó redundante é promovido a nó principal.

Clusters com balanceamento de carga distribuem dinamicamente o processamento e o tráfego de rede, impedindo a sobrecarga de um dos nós.

O mecanismo de substituição de um nó por outro, após a ocorrência de uma falha, é chamado de *failover*. O *failover* pode ocorrer em duas configurações: ativo/passivo e ativo/ativo. Na configuração ativo/passivo, um ou mais nós executam aplicativos, enquanto outros nós ficam no modo de espera, preparados para assumir o processamento em caso de falha de um dos nós principais. Na configuração ativo/ativo, todos os nós ficam processando aplicações permanentemente, sendo que no caso de falha de um nó, a atividade desenvolvida até então é distribuída pelos demais nós do sistema de *clusters*.

Trata-se de estabelecer a relação custo/benefício mais apropriada, pois no caso da configuração ativo/passivo não há perda de desempenho em caso de falha, mas há recursos que ficam sub-utilizados a maior parte do tempo. No caso da configuração ativo/ativo, não há recursos sub-utilizados, mas o desempenho do sistema sofre uma degradação no caso de problemas em um ou mais nós.

Outra forma de implementação de redundância ocorre por meio da técnica RAID – *Redundant Array of Inexpensive Disks*, que provê a redundância de discos rígidos que armazenam os dados da aplicação. Maiores detalhes desta técnica são fornecidos no item 5.1.5.

3.4.2. Técnicas de Armazenamento e Recuperação de Dados

Neste item são apresentadas as tecnologias de armazenamento e recuperação de dados utilizadas em Sistemas de Informação, compreendendo a descrição dos principais aspectos referentes às tecnologias de bases de dados, data warehouse e data mining.

3.4.2.1. Bases de Dados

Uma Base de Dados constitui-se em um sistema computadorizado de armazenamento de coleções de registros, cujo propósito é o de armazenar informações e permitir ao usuário a busca e atualização dessas mesmas informações.

Bases de Dados estão presentes em praticamente todos os sistemas computadorizados atualmente desenvolvidos. Rara é a aplicação que não necessita preservar dados sobre o sistema sob seu controle e supervisão. Não apenas o número de aplicações é crescente, mas também a importância das Bases de Dados. Além de ter que apresentar funcionamento ininterrupto, ou seja, as 24 horas do dia, pelos 7 dias da semana, uma interrupção ou um problema em uma Base de Dados pode significar um prejuízo muito grande à organização detentora da mesma.

Além desse aspecto, também é extremamente importante que se assegure um bom desempenho às aplicações de Bases de Dados.

Para que seja feita a implementação de uma Base de Dados é utilizado um Sistema Gerenciador de Bases de Dados (SGBD), uma linguagem ou um ambiente de programação e normalmente uma interface com o ambiente Web, visto que praticamente todas as Bases de Dados atualmente desenvolvidas apresentam acesso via Internet (SILBERSCHATZ et al., 2002).

Uma distinção que se faz necessária é com relação aos conceitos de dados e de informações. Dados representam o conteúdo armazenado, enquanto que informações implicam na atribuição de um significado a esse conteúdo. Por exemplo, uma coleção de valores, tais como 55, 48, 46, 33, simplesmente representa um conjunto de números. Ao se dizer que tais valores representam as idades de pessoas, estará se

atribuindo um significado aos dados, que assim passam a carregar algum tipo de informação.

No linguajar mais informal, é feita uma confusão na terminologia, utilizando-se o termo Base de Dados para designar o Sistema Gerenciador de Bases de Dados, mais os dados propriamente ditos, quando na realidade os dados propriamente ditos não compõem o Sistema Gerenciador, conforme apresentado na figura 3.5.

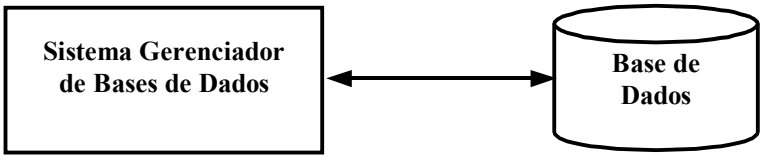

Figura 3.5 – Base de Dados e Sistema Gerenciador

O Sistema Gerenciador de Bases de Dados é o conjunto de programas responsáveis pelo gerenciamento dos dados contidos em uma base de dados, permitindo o acesso aos dados (DATE, 2000).

A função principal do Sistema Gerenciador de Bases de Dados é a de simplificar e facilitar o acesso aos dados. O Sistema Gerenciador se constitui no software que trata todas as requisições de acessos à base de dados, representando uma interface entre os dados armazenados e os programas de aplicação e consultas submetidas ao sistema.

Os dados são persistentes, ou seja, uma vez aceitos pelo Sistema Gerenciador de Bases de Dados, só podem ser removidos por alguma solicitação explícita ao próprio Sistema Gerenciador de Bases de Dados.

As principais tarefas de um Sistema Gerenciador de Bases de Dados são (KROENKE, 1998):

- Interagir com o Gerenciador de Arquivos: dados estão armazenados em disco, utilizando o sistema de arquivos, normalmente integrante de um Sistema Operacional; o Sistema Gerenciador de Bases de Dados traduz as instruções da linguagem de processamento de dados, em comandos de baixo nível do sistema de arquivos, possibilitando a troca de dados;

- Garantia da Integridade: os valores de dados armazenados na Base de Dados podem ter de satisfazer a certos tipos de restrições ou condições e o Sistema Gerenciador de Bases de Dados deve verificar se as atualizações ocorridas respeitam todas as regras de integridade estabelecidas;
- Garantia da Segurança: nem todo usuário necessita ou deve ter acesso a todo conteúdo ou a todas operações de uma Base de Dados; daí a necessidade de controle de acesso aos usuários;
- Recuperação e *Backup*: em caso de falha em módulos do computador (disco, memória, etc.) devem existir mecanismos de recuperação que possibilitem restaurar a Base de Dados à situação original (antes da falha). Se isso não for possível, deve haver facilidades de recuperação por meio de cópias de segurança (*backup*);
- Controle de Concorrência: diversos usuários podem utilizar uma Base de Dados concorrentemente, sendo que a consistência dos dados não pode ser violada. Esta característica faz parte do controle da interação entre usuários concorrentes.

3.4.2.2. Data Warehouse

Um Data Warehouse se constitui em uma base de dados especializada, montada, principalmente, a partir de dados oriundos de diversas bases de dados operacionais presentes em uma organização, permitindo a centralização e a padronização de informações presentes em seus diversos segmentos. Com a montagem de um ambiente separado do ambiente operacional, torna-se possível a realização de pesquisas analíticas sobre essas informações.

A razão para a montagem de um novo ambiente, além das Bases de Dados já existentes, está no fato que os dados dos diversos segmentos não estão, normalmente, relacionados entre si, apresentando discrepâncias em seus significados. Dessa forma, os dados não teriam grande utilidade como recurso estratégico no processo de tomada de decisões. Além da não padronização dos dados, estes se encontram espalhados pelos diversos ambientes computacionais da organização e o acesso constante a esses ambientes iria atrapalhar o processamento diário ou convencional da organização.

Alguns dos segmentos com uso mais intenso de Data Warehouse são os setores de telecomunicações, bancos, manufatura, assistência médica, universidades, seguros, dentre outros. Dentro desses segmentos, as áreas de aplicação mais comuns são as de Gerenciamento de Risco, Análise Financeira, Programas de Marketing, Tendências de Lucro com Produtos, Análise de Aquisição, Gerenciamento do Ativo e Administração do Relacionamento com o Cliente.

O objetivo fundamental de um banco de dados do tipo data warehouse é servir de base para análise e consulta (KIMBALL, 1998). Em primeiro lugar há as análises do tipo estratégico, onde se busca um apoio objetivo no conjunto de informações para o processo de tomada de decisões. Em outro nível, situam-se análises táticas e gerenciais, onde o tipo de decisão não é tão importante, porém mais freqüente. Não faz parte essencial da missão de um sistema de data warehouse dar suporte à tomada de decisão no nível operacional, onde o que se busca é a realização de uma transação e não a aquisição de um conhecimento que apóie a gestão das atividades da organização (WILLENSES, 2002).

As consultas que são feitas a um sistema de data warehouse são muito exigentes em termos de volume, pois consolidam grandes massas de dados e são pouco exigentes em termos de tempo de resposta, visto não serem ações corriqueiras, sendo realizadas por uma pequena parcela da organização. Outras características importantes das consultas é que são muito variadas e pouco previsíveis, além de não focalizam itens individuais de informação, mas consolidações destes sob diversos aspectos. (INMON, 1996).

A necessidade de atender bem às análises e ao tipo de consulta descrito, traz ao sistema de data warehouse algumas características muito próprias (KIMBALL, 1998):

- Armazenamento de dados históricos, não apenas dados atuais;
- Armazenamento de dados externos à organização;
- Armazenamento de dados integrados de toda (ou de grande parcela) da organização;

- Organização dos dados segundo a perspectiva do negócio como um todo, e não pautada pelas peculiaridades dos diferentes processos executados rotineiramente;
- Apresentação de uma forma facilmente compreensível das interdependências existentes entre os dados;
- Facilidade de obtenção de dados sumarizados;
- Um grande volume de dados.

Não necessariamente um sistema de data warehouse precisa ter todas as propriedades listadas acima. É possível imaginar que algumas das bases não possuam dados históricos ou que outra base armazene apenas um pequeno volume de dados. Assim, as características listadas devem ser entendidas como pertinentes ao sistema de data warehouse como um todo, e não necessariamente a cada um de seus componentes.

A figura 3.6 representa esquematicamente o fluxo de dados em um Data Warehouse. Nesta figura há uma caixa chamada ETL, que representa a etapa de transferência de dados do ambiente operacional para o Data Warehouse. Esta etapa é composta por três fases, que são a extração dos dados, sua transformação e a carga no Data Warehouse (ETL – *Extraction, Transformation Load*).

Os Data Marts vistos na figura 3.6 constituem-se em porções de dados do Data Warehouse especializadas, por exemplo, por região, por departamentos ou por áreas da empresa.

Uma aplicação mais recente que os sistemas de data warehouse vêm tendo é o armazenamento e a correspondente pesquisa de dados originados de seqüência de visitação de sites da Internet, visando identificar tendências e preferências de usuários. Kimball (2000) dá a este tipo de implementação o nome de Data Webhouse.

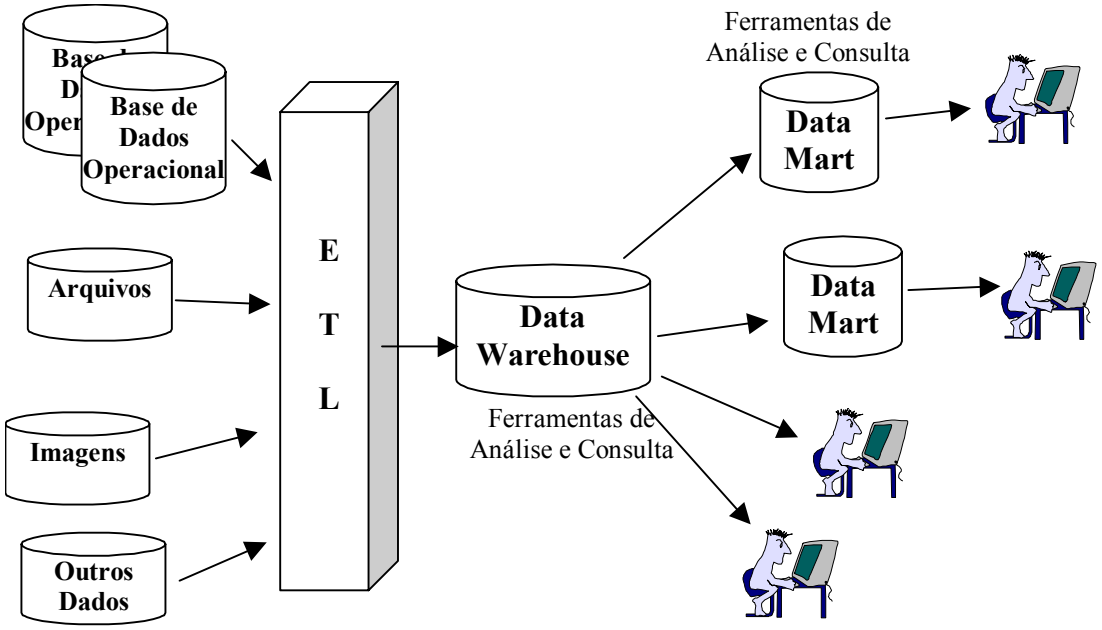

Figura 3.5 – Diagrama Esquemático da Montagem de um Data Warehouse

Finalmente, os Data Warehouses têm seus dados explorados, principalmente, através das chamada ferramentas OLAP - *OnLine Analytical Process*, cujo objetivo é realizar a análise multidimensional, ou seja, a habilidade de processar dados que tenham sido agregados em várias categorias ou dimensões (RUSSOM, 2000).

As ferramentas OLAP permitem que analistas, gerentes e executivos obtenham, de maneira rápida, consistente e interativa, acesso a uma ampla variedade de possíveis visualizações de informações, de maneira que reflitam a dimensão real do empreendimento, do ponto de vista do usuário

3.4.2.3. Data Mining

Na maioria das ferramentas utilizadas para analisar um Data Warehouse, o usuário já sabe ou tem idéia do que irá consultar ou comprovar. Essa abordagem depende do usuário e pode impedir que padrões não diretamente visíveis nos dados sejam encontrados, uma vez que um analista não terá condições de imaginar todas as possíveis relações e associações existentes. Por isso, faz-se necessária a utilização de técnicas de análise dirigidas por computador, que possibilitem a extração automática (ou semi-automática) de conhecimentos total ou parcialmente novos (GANTI et al., 1999), (HEDBERG, 1995).

Daí a necessidade da utilização da tecnologia de Data Mining, cujo objetivo é o de extrair informações não evidentes da enorme massa de dados que compõem um Data Warehouse. Este é um ambiente extremamente adequado para o utilização do Data Mining, pois os dados já estão em formatos padronizados, sem a existência de problemas comuns encontrados em múltiplas bases de dados, tais como a não existência de valores, valores nulos ou a não padronização dos dados (CARVALHO, 2001).

O processo de aplicação do Data Mining propriamente dito é ilustrado na figura 3.7. Em um ambiente mais geral, os dados têm de, eventualmente, passar por uma fase de pré-processamento, cujo objetivo é o de proporcionar uma padronização dos mesmos. Após isto, é realizada a procura por padrões existentes nos dados, através da aplicação de simples consultas, de técnicas estatísticas ou da inteligência artificial. Os resultados são submetidos à revisão por parte de um analista que pode solicitar novas buscas nos dados, até que sejam obtidas as informações necessárias. Quando o analista considerar que o resultado obtido é satisfatório, submete as regras obtidas à interpretação de resultados que vão auxiliar no processo de tomada de decisões.

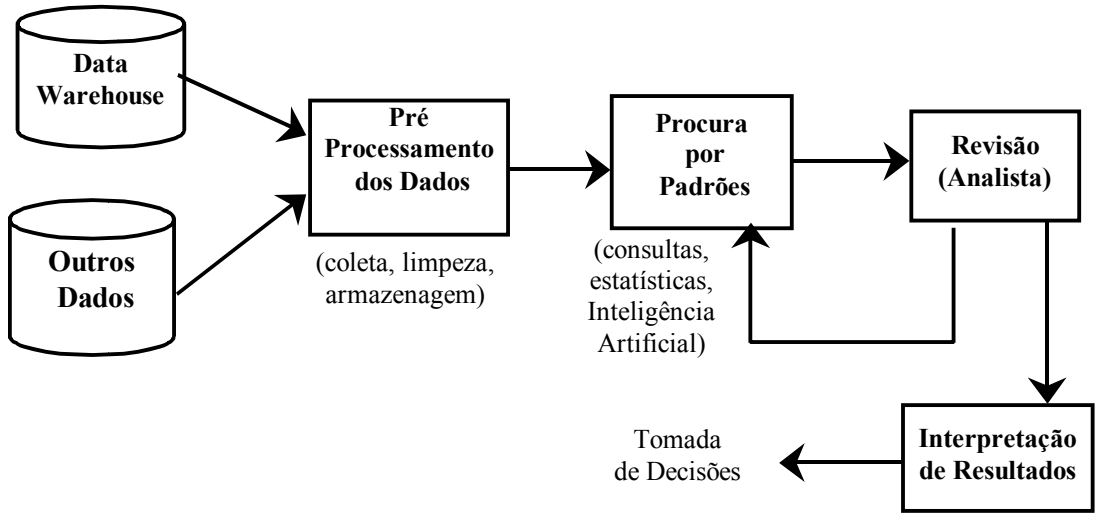

Figura 3.7 - Fases do Data Mining

Há muitos campos de aplicação para o Data Mining. Um deles é a identificação de padrões de transferência de fundos com vistas à detecção de lavagem de dinheiro ou de fraudes, utilizada principalmente pela área governamental. Em supermercados e em grandes magazines, o Data Mining pode ser usado para o cruzamento de dados

pessoais, preferências individuais e compras realizadas, visando obter as melhores formas de organização e exposição de mercadorias nas lojas (WESTPHAL; BLAXTON, 1998).

Nas áreas de geologia e de astronomia, o Data Mining pode ser utilizado para a identificação de padrões não detectados ou não percebidos de fotos de satélites ou de telescópios, conforme o caso.

Na medicina, as técnicas de Data Mining podem ser utilizadas no cruzamento de dados de sintomas, doenças, diagnósticos, tratamentos e exames, tendo como objetivo a identificação de relacionamentos entre esses diversos fatores.

Na área de negócios pode-se utilizar o Data Mining para se efetuar o planejamento de estratégias de investimento ou então para a identificação de novas tendências de mercado. Outra utilização se faz por empresas de telefonia celular que, baseadas em padrões de uso dos telefones e outros fatores de mercado, obtêm previsões de quais clientes estão propensos a migrar para os concorrentes.

Exemplos de aplicação das técnicas de Data Mining não param aí. Pode-se citar sua aplicação na área esportiva, na área jurídica, na identificação de padrões de compras com cartões de crédito, e assim por diante, apenas para destacar as principais aplicações.

A forma de implementação de Sistemas de Informação, descrita neste item, é uma das etapas importantes no processo de garantia da Segurança de Informação, que, no entanto, não é mantida apenas pela aplicação de técnicas apropriadas de projeto, mas também por intermédio de técnicas de análise da Segurança de Informação, descritas a seguir.

3.5. Análise de Segurança de Sistemas de Informação

A Análise de Segurança de Sistemas de Informação é feita observando-se as ameaças, riscos e impactos que possíveis invasões ou problemas nos sistemas possam causar à sua operação.

As principais fases componentes de uma Análise de Segurança de Sistemas de Informação são a classificação das informações, a análise de ameaças e a análise de riscos e impactos.

Desta forma, neste item analisam-se tais aspectos, iniciando-se por uma classificação das informações, importante para a definição do grau de proteção necessário.

3.5.1. Classificação das Informações

Tendo em vista que o grau de proteção exigido varia de acordo com o tipo de informação, é necessário estabelecer uma classificação dos tipos de informações disponíveis ou existentes em uma organização. Uma das classificações mais utilizadas é a seguinte (DIAS, 2000):

- Públicas ou de Uso Irrestrito: são informações que podem ser divulgadas livremente a qualquer pessoa, sem nenhuma implicação para a instituição, como por exemplo material de divulgação institucional da empresa;
- Internas: tal tipo de informação não deve ser divulgado fora da instituição, mas se isso ocorrer, as conseqüências não são críticas, como por exemplo informações gerais internas;
- Confidenciais: representam informações sigilosas sobre o andamento de projetos e negócios da empresa, sendo que mesmo o acesso interno é controlado, como por exemplo, dados de clientes e de projetos;
- Secretas: constituem-se em informações altamente confidenciais e de acesso extremamente controlado, mesmo dentro da empresa, como por exemplo, arquivos de senhas e de dados financeiros.

3.5.2. Análise de Ameaças

Ameaças se constituem em perigos potenciais aos recursos de um sistema computacional e a seu Sistema de Informação. Portanto, para que se possa proteger as informações contidas em um Sistema de Informação, é necessário que se conheçam as ameaças potenciais, de modo a que se possa prever a proteção apropriada.

Uma ameaça é composta por eventos ou atividades indesejáveis, tais como o furto de informações, a ocorrência de um incêndio ou o ataque por um vírus de computador.

A concretização de uma ameaça pode desabilitar, danificar ou excluir um recurso computacional do Sistema de Informação, seja esse recurso constituído pela informação em si ou por qualquer componente de hardware ou software do sistema computacional.

As ameaças existentes procuram explorar as deficiências ou vulnerabilidades de um sistema. Um sistema pode estar exposto a vulnerabilidades humanas, físicas, naturais, de software e de comunicação de dados (DIAS, 2000).

Vulnerabilidades humanas estão ligadas à falta de treinamento, à falta de comprometimento com a organização e a possíveis compartilhamentos de informações por funcionários da própria organização. Vulnerabilidades físicas referem-se ao não policiamento de salas e à não existência de barreiras físicas com relação ao local onde está instalado o hardware do Sistema de Informação.

Vulnerabilidades naturais são provocadas por eventos tais como terremotos, enchentes e condições de temperatura e umidade inadequadas do ambiente computacional. Vulnerabilidades do software ficam por conta de problemas no sistema operacional e nos programas aplicativos. Por fim, a vulnerabilidade na comunicação de dados está ligada à não existência de mecanismos de proteção na comunicação de dados entre máquinas.

Se uma ameaça potencial conseguir, de fato, superar as barreiras de proteção de um Sistema de Informação, através de seus pontos vulneráveis, é necessário que se

realize uma análise do impacto decorrente da concretização das ameaças. A cada ameaça pode ser associada uma probabilidade, que representa a chance da concretização de suas conseqüências.

Ameaças podem ser classificadas em acidentais ou deliberadas. Uma ameaça do tipo acidental ocorre em virtude de falhas no hardware, por erros de programação ou desastres naturais. Uma ameaça do tipo deliberada ou proposital ocorre em razão de tentativas de acesso não autorizado ao sistema e pode ser classificada nos tipos passivo e ativo. Em ameaças deliberadas do tipo passivo ocorre uma invasão ao sistema e são realizadas leituras a seus dados, sem que ocorra sua alteração. Já em uma ameaça deliberada do tipo ativo, ocorre a alteração proposital dos dados.

O vazamento de informações é uma ameaça do tipo deliberada, consistindo na obtenção de informações confidenciais ou secretas por pessoas ou sistemas não autorizados.

A violação da integridade dos dados pode ocorrer por intermédio de ameaças acidentais ou deliberadas. Em ambas as situações, os dados são alterados de forma a violar as regras de consistência a eles impostas.

A indisponibilidade de um Sistema de Informação consiste no impedimento de acesso, deliberado ou acidental, aos recursos computacionais por usuários autorizados.

Finalmente há as ameaças deliberadas do tipo programado, que se constituem em códigos de software que se alojam no sistema com o intuito de comprometer sua segurança, alterando seu comportamento, violando controles de segurança, alterando ou destruindo dados. A ameaça programada mais comum é constituída pelos vírus de computador, que são representados por programas projetados para se replicarem e se espalharem de um computador a outro, atacando programas instalados.

3.5.3. Análise de Riscos e de Impactos

Pode-se definir o risco como a probabilidade da ocorrência de qualquer evento que possa afetar as atividades de uma organização, impedindo que se atinjam os objetivos desejados ou planejados em termos dos negócios a serem realizados.

A análise de risco compreende a análise das ameaças que possam estar presentes, das vulnerabilidades de um sistema e dos impactos decorrentes da concretização de ameaças.

Só é possível adotar corretamente as medidas preventivas desde que se conheçam as ameaças potenciais, como tais ameaças podem explorar as vulnerabilidades do sistema e quais são os possíveis impactos, tendo em vista as ameaças existentes.

Os principais impactos a que os sistemas computacionais estão sujeitos são: modificação dos dados, indisponibilidade de sistemas vitais, divulgação de informações confidenciais, perda de credibilidade da instituição, possibilidade de abertura de processos legais contra a instituição e perda de clientes para a concorrência (BYRNES; KUTNICK, 2002)..

A análise de risco constitui-se no processo de identificação e avaliação dos fatores de risco presentes, de forma antecipada, possibilitando uma visão do impacto negativo, possivelmente causado aos negócios. A realização da análise de risco possibilita a identificação do valor e do tipo de investimento necessário para a prevenção de ataques contra a informação.

O custo é um dos fatores a ser considerado quando da análise de risco, pois se o custo para se combater uma ameaça potencial for superior a um possível dano decorrente dessa ameaça, talvez não seja aconselhável tomar qualquer medida preventiva.

Não é possível a eliminação total dos riscos de um Sistema de Informação, ou seja, desenvolver um sistema com risco zero. No entanto, os riscos podem ser reduzidos através da adoção de medidas de segurança, diminuindo-se a probabilidade de sua ocorrência, mas nunca os anulando por completo (DIAS, 2000).

Após terem sido definidos os principais conceitos relativos às ameaças, riscos e impactos presentes em Sistemas de Informação, faz-se necessária a aplicação requisitos mínimos a seus projetos. Isto é obtido através da aplicação de algumas normas especialmente desenvolvidas, visando o projeto e implementação de Sistemas de Informação, conforme descrito a seguir.

3.6. Normas Utilizadas em Sistemas de Informação

Neste item são apresentadas algumas das normas existentes na área de Tecnologia da Informação, e que abrangem o aspecto da Segurança de Informação.

3.6.1. Norma NBR ISO/IEC 17799

Esta norma da ABNT (Associação Brasileira de Normas Técnicas) tem sua origem na norma ISO/IEC 17799:2000, que por sua vez se originou da primeira parte da norma britânica BS7799, do *British Standard Institute*. A ABNT homologou a NBR ISO/IEC 17799 - Tecnologia da Informação: Código de Prática para a Gestão da Segurança de Informação - em 2001 (ABNT, 2001). A segunda parte da norma britânica BS7799 refere-se à especificação de sistemas de gestão para a Segurança de Informação e vem sendo objeto de estudos por parte do ISO (*International Standards Organization*) para a sua adoção a nível mundial.

O objetivo desta norma é o de fornecer recomendações para a gestão da Segurança de Informação, para assegurar a continuidade da operação de sistemas computacionais e minimizar danos aos negócios, prevenindo e diminuindo o impacto de incidentes de segurança. Outros objetivos são o de prover uma base comum para o desenvolvimento de práticas de segurança nas organizações, bem como prover segurança nos relacionamentos entre empresas.

Na NBR ISO/IEC 17799, a Segurança de Informação é caracterizada pela preservação dos atributos de confidencialidade, integridade e disponibilidade. Por confidencialidade a norma se refere às informações cujo acesso só pode ser feito por parte de quem possuir autorização para tal. A integridade refere-se à garantia da

precisão das informações e a disponibilidade está relacionada à garantia de que os usuários autorizados tenham acesso, quanto necessário, à informação.

A norma NBR ISO/IEC 17799 define a Segurança de Informação como a proteção contra ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimento e oportunidades.

Os princípios colocados na norma NBR ISO/IEC 17799 relacionam-se aos seguintes aspectos:

- Política de Segurança: visa direcionar e apoiar a segurança, gerando-se um documento da Política de Segurança na empresa;
- Organização da Segurança: tem como meta gerenciar a Segurança de Informação, definindo-se responsabilidades e identificando-se os riscos;
- Classificação dos Ativos: pretende atribuir o nível de proteção adequado aos ativos, montando-se um inventário e guias para sua classificação;
- Segurança em Pessoas: seu objetivo é o de reduzir riscos provenientes de erros humanos, roubo, fraude e uso impróprio das informações, através de seleção e política de recursos humanos, bem como capacitação de usuários;
- Segurança Física e do Ambiente: visa prevenir acessos não autorizados que possam danificar e interferir nos locais onde a empresa opera, delimitando áreas protegidas, implantando a política de mesa e tela limpas;
- Operações e Comunicações: tem como finalidade garantir a operação segura e correta dos recursos de processamento da informação, através da administração da rede e de proteção contra programas estranhos ao Sistema de Informação;
- Controle de Acesso: visa controlar o acesso à informação, através do gerenciamento de acessos de usuários;
- Desenvolvimento e Manutenção de Sistemas: sua meta é a de garantir que a segurança seja parte integrante dos Sistemas de Informação, através da segurança em sistemas aplicativos;

- Continuidade dos Negócios: tem como objetivo reagir às falhas de segurança nas atividades do negócio, protegendo processos críticos de um desastre;
- Conformidade: visa evitar a violação de qualquer lei criminal ou cível, estatutos, regulamentações ou obrigações contratuais.

3.6.2. Norma ISO/IEC 15408-1

Esta norma - *Information Technology – Security Techniques – Evaluation Criteria for IT Security* - é editada pelo ISO/IEC (*International Organization for Standardization/International Electrotechinical Commision*), tendo sido aprovada em 1999 (IEC, 1999). Sua finalidade é a de definir como os chamados Critérios Comuns (*Common Criteria* - CC) devem ser usados para a avaliação de propriedades de segurança de informação em produtos e sistemas que envolvam Tecnologia da Informação.

Esses Critérios Comuns provêm um conjunto comum de requisitos às funções de segurança da Tecnologia de Informação, abrangendo, dentre outros, proteção contra acessos indevidos, modificações ou exclusões não autorizadas de informações.

O público alvo para esta norma é composto por consumidores, desenvolvedores e avaliadores. Os consumidores ou usuários podem utilizar resultados de avaliações para decidir qual ou quais produtos irão incorporar em seus sistemas. Desenvolvedores utilizam a norma para preparar seus produtos de forma adequada aos requisitos mínimos de Segurança de Informação. Finalmente, avaliadores utilizam a norma para poderem exercer os julgamentos necessários sobre produtos desenvolvidos.

A norma é dividida em três partes, a primeira com uma introdução e a apresentação de um modelo geral de avaliação, a segunda estabelece um conjunto de requisitos funcionais e a terceira um conjunto de requisitos de segurança.

3.6.3. Norma NIST 800-30

Esta norma - Risk Management Guide for Information Technology Systems - é editada pelo NIST (*National Institute of Standards and Technology*), órgão americano, tendo sido aprovada em 2001 (NIST, 2001). Sua finalidade é a de prover uma base para o desenvolvimento de um programa de gerenciamento de risco, contendo definições e um guia prático para detectar e diminuir riscos em Sistemas de Informação.

O público alvo desta norma vai desde a alta gerência de uma organização, até o grupo encarregado da garantia da qualidade, passando por todo o pessoal técnico.

Esta norma fornece uma visão geral sobre o gerenciamento de riscos, sua importância e sua integração no ciclo de desenvolvimento de sistemas. A norma estabelece ainda as funções de cada um dos responsáveis pelo sistema, no que diz respeito ao gerenciamento de risco.

A norma descreve nove passos para a determinação dos riscos, que são: caracterização do sistema, identificação de ameaças, identificação de vulnerabilidades, análise dos controles de segurança, determinação das probabilidades das ameaças identificadas, análise de impacto, determinação do nível de risco, geração de recomendações e geração de documentação com os resultados.

A norma apresenta também um questionário para a realização de entrevistas, cuja finalidade é a detecção de áreas de risco na organização.

3.6.4. Orange Book

No fim dos anos 70 a *National Security Agency* (NSA), agência americana estabeleceu requisitos formais a serem cumpridos para a Segurança de Informação, publicados em uma série de documentos conhecidos como *Rainbow Books*. O mais significativo desses é o *Orange Book*, que teve sua primeira edição em 1983 e uma revisão em 1986 (HUNTER, 2001). A denominação oficial do Orang*e Book* é TCSEC (*Trusted Computer System Evaluation Criteria*).

O *Orange Book* apresenta as características requeridas para sistemas computacionais, onde a Segurança de Informação é uma exigência. O *Orange Book* apresenta 27 propriedades desejáveis para a Segurança de Informação, dentre elas auditoria, gerenciamento de configurações, documentação, especificação e verificação, controle de acesso, identificação e autenticação, testes de segurança e recuperação. O *Red Book* interpreta os princípios e critérios do *Orange Book* para ambientes do tipo cliente/servidor.

O *Orange Book* define 7 níveis de segurança: D, C1, C2, B1, B2, B3 e A1. O nível D, chamado de Proteção Mínima, não requer nenhuma característica especial de segurança. O nível mais exigente é o A1, chamado de Projeto Verificado, que exige identificação de usuários através de senhas, com níveis de acesso individualizados, além de processos de validação do projeto de segurança perante suas especificações.

Seguindo a linha do *Orange Book*, a comunidade européia criou o padrão ITSEC – IT *Security Evaluation Criteria*, relativo à Segurança de Informação, formulado por França, Alemanha, Holanda e Reino Unido.

3.6.5. SSP - System Security Policy

Esta é uma recomendação do governo britânico, visando a proteção nas fases de processamento, armazenamento e transmissão de informações em sistemas computacionais que tratem de informações consideradas secretas. Os sistemas que realizam essa tarefa são regulamentados pelo DSO (*Departamental Security Officer*), que verifica se os mesmos não representam riscos à segurança nacional. Para que se obtenha a permissão de operação, o responsável pelo sistema computacional deve fornecer dados relativos ao escopo do sistema, aos requisitos de Segurança de Informação, às medidas para a implementação de tais requisitos, bem como a alocação de responsabilidades. A esse conjunto de tópicos dá-se o nome de *System Security Policy* – SSP (HUNTER, 2001).

Pode ser requerida a avaliação, por consultores independentes, visando a certificação dos aspectos da Segurança de Informação. Tais consultores necessitam de informações sobre:

- Detalhamento dos aspectos técnicos do SSP, também conhecido como *System Electronic Information Security Policy* – SEISP;
- Documento de projeto do sistema das partes referentes à segurança de informações;
- Código fonte das seções críticas, ou seja, partes do código que contenham funções de Segurança de Informação.

O propósito da certificação é assegurar que o projeto reflita os requisitos SEISP e que o código implemente corretamente as especificações do projeto.

Neste item foram descritas as principais normas utilizadas para a garantia da Segurança de Informação. Finalizando este capítulo, no próximo item descrevem-se as principais aplicações que os Sistemas de Informação encontram atualmente.

3.7. Principais Aplicações de Sistemas de Informação

A gerência das organizações está engajada em um processo contínuo de tomada de decisões. No ambiente de negócios extremamente competitivo dos dias atuais, o custo de se cometer um erro em uma decisão é muito grande, tendo em vista a complexidade cada vez maior das decisões gerenciais e a magnitude também crescente das operações. As decisões devem ser tomadas com rapidez cada vez maior.

A utilização de ferramentas computacionais nesse ambiente gerencial propiciou a superação de limites cognitivos do ser humano, tanto no que se refere ao processamento, quanto ao armazenamento das informações.

Pode-se dizer que a economia vem passando por um processo de transformação, tendo cada vez mais importância o conhecimento e a informação. Novos produtos e serviços são oferecidos a velocidades cada vez maiores. Os produtos vêm tendo seu ciclo de vida encurtado e o tempo de geração de respostas assume papel de importância crescente. Os empreendimentos são cada vez mais descentralizados e a independência de localização dos dados torna-se um fator primordial.

A informação representa um dos principais recursos à disposição das organizações e deve ser gerenciado como qualquer outro recurso. A figura 3.8 ilustra o processo de gerenciamento da informação, que sofre o processamento necessário, é armazenada e utilizada tanto para o controle geral da organização, quanto para as atividades estratégicas de gerenciamento. Portanto, o gerenciamento da informação compreende sua obtenção, sua disponibilização na forma e tempo apropriados e sua substituição quando de sua obsolescência.

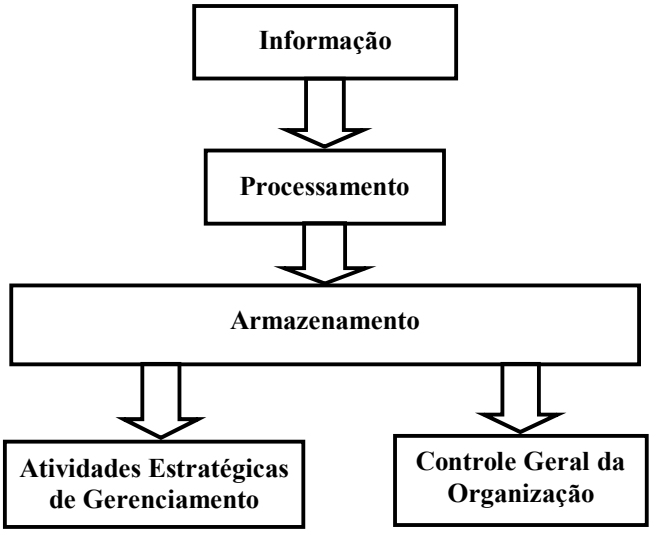

Figura 3.8 - Fluxo de Gerenciamento da Informação

Tendo em vista a grande importância dos Sistemas de Informação nos dias atuais, nos próximos itens são descritas algumas de suas principais aplicações.

3.7.1. Sistemas de Suporte à Decisão

As empresas vêm acumulando quantidades enormes de informações geradas por seus sistemas de aplicações, extremamente importantes às organizações. A utilização desse grande volume de dados permite que se obtenham informações para o suporte à tomada de decisões, visando, por exemplo, detectar tendências de consumo, prever aumento ou redução da produção, regular estoques, lançar campanhas publicitárias de incentivo ao consumo, medir a eficiência do pessoal, etc. (TURBAN; ARONSON, 1998).

A utilização do ambiente operacional ou de produção com a finalidade de servir a essa tarefa de suporte à decisão não é conveniente, pelo fato de sobrecarregar o processamento desse ambiente com consultas a muitos registros, podendo atrapalhar as operações diárias da organização. Daí a razão em se montar um ambiente isolado do ambiente operacional, proporcionando acesso contínuo por parte dos usuários, sem afetar as operações convencionais da empresa.

O meio utilizado para o armazenamento dessas informações é o Data Warehouse, cuja descrição é feita no item 3.4.2.2. Dessa forma, as decisões da corporação podem considerar todas as informações disponíveis, de maneira eficiente e organizada (MCLEOD, 1995). Esta é a base para o desenvolvimento dos Sistemas de Suporte à Decisão (*Decision Support Systems* – DSS), que se constituem em sistemas interativos baseados em computador, cujo objetivo é auxiliar tomadores de decisão, na resolução de problemas estratégicos não estruturados. Os Sistemas de Suporte à Decisão acoplam recursos intelectuais humanos com as capacidades do computador, sempre visando a melhoria na qualidade das decisões.

Cada vez mais os Sistemas de Suporte à Decisão vêm demonstrando sua utilidade em proporcionar ferramentas à gerência e à diretoria das empresas, agilizando e melhorando a acurácia no processo estratégico de tomada de decisões. Com o ambiente cada vez mais competitivo, e com o crescente número de alternativas, o custo de uma decisão incorreta ou tomada com atraso é muito grande, podendo significar grandes perdas.

Os Sistemas de Suporte à Decisão são Sistemas de Informação especialmente desenvolvidos para suportar a solução de problemas de gerenciamento, propiciando melhor qualidade nas decisões e aumentando a produtividade das empresas. Outras características são a de melhorar a satisfação de clientes e funcionários, evitar ou reduzir possíveis efeitos negativos que se façam presentes e identificar oportunidades, além de prover visão organizacional das operações. Os Sistemas de Suporte à Decisão devem possuir interface extremamente amigável, prover controle e rastreamento efetivo e fornecer suporte a decisões inter-relacionadas.

As fases presentes na tomada de decisões são a definição do problema, a realização de atividades de decisão, a implementação das decisões tomadas e eventuais revisões (TURBAN; ARONSON, 1998).

A definição do problema consiste na busca e avaliação de informações sobre o problema. Na atividade de decisão são realizadas atividades de criação, desenvolvimento e análise de possíveis soluções, bem como são identificadas e analisadas alternativas e selecionada a melhor solução. As duas últimas fases consistem na implementação da solução, seu acompanhamento e eventuais atividades de revisão da solução implementada.

3.7.2. Gerenciamento de Relações com os Clientes

O Gerenciamento de Relacionamento com os Clientes, ou *Customer Relationship Management* - CRM, tem como objetivo oferecer a oferta certa, no momento certo e utilizando o canal correto (TEKLITZ; McCARTHY, 1999).

Tendo em vista tal definição, as principais funções que se colocam para o CRM são obter aproximação e melhor relacionamento com os clientes, reduzir o custo de obtenção de novos clientes, procurar a obter a fidelidade dos clientes obtidos, bem como deslocar a interface cliente-empresa para meios mais efetivos de custo mais baixo. Outras funções desempenhadas pelo CRM são obter perfis exatos dos clientes, determinar a combinação certa de produtos, serviços, vendas e *marketing*, bem como reter os clientes, conseguindo sua lealdade.

É importante frisar que um projeto de implantação de um CRM deve estar inserido dentro da cultura geral da organização, tendo em vista que o foco ou orientação principal passa a ser o cliente, ou seja, passa-se a ter uma empresa orientada ao cliente.

A análise do cliente envolve a obtenção de informações sobre seu histórico de consumo, estilo de vida e informações pessoais, tendo como objetivos a determinação de seu perfil, atribuição de pontuações a formas de *marketing* e medição do grau de retenção e lealdade dos clientes.

Há três vertentes do CRM, o analítico, o operacional e o colaborativo. O CRM analítico tem como objetivo identificar como são os clientes e quais têm probabilidade de serem os mais rentáveis e que devem merecer um tratamento personalizado. O CRM analítico atua como suporte do CRM operacional, proporcionando uma seleção mais precisa dos grupos de clientes.

O CRM operacional objetiva criar os mecanismos que propiciem a operacionalização das estratégias definidas quando do projeto do CRM e da aplicação do CRM analítico. Dentre alguns mecanismos que podem ser citados estão a implantação de Centrais de Atendimento e sites de comércio eletrônico.

Por fim, o CRM colaborativo atua como suporte ao CRM operacional e ao CRM analítico, contendo as ferramentas de automação e integrando as formas de contato utilizadas pelo cliente na comunicação com as empresas.

O ciclo de CRM envolve quatro fases, que são compreender e diferenciar os clientes, desenvolver e personalizar produtos, interagir com os clientes e, finalmente, conseguir retê-los (TEKLITZ; McCARTHY, 1999).

A fase de compreensão e diferenciação consiste em conhecer cada cliente e reconhecê-lo em suas interações com a empresa, possibilitando a categorização dos clientes, levando em conta seu valor e suas necessidades junto à empresa.

O desenvolvimento e a personalização têm como objetivo desenvolver produtos, serviços e canais para atender às necessidades do cliente e, na medida do possível, personalizados por grupos de clientes ou até individualmente para os clientes mais importantes.

Na terceira fase realiza-se uma interação com os clientes, fortalecendo sua relação com a empresa, visando a manutenção da continuidade dos negócios. O valor de um negócio concretizado não significa apenas o produto e preço, mas também a qualidade dos produtos e serviços, e o comprometimento mútuo.

Finalmente, a última fase consiste em se adquirir novos clientes e reter aqueles de maior valor agregado. A retenção de clientes começa com uma aquisição bem feita.

Muitos projetos de CRM têm início pela escolha da tecnologia de software e de hardware. Esta não é a forma correta de ação, visto que CRM é uma filosofia de trabalho e que a tecnologia é importante, mas não é seu foco central.

O CRM não se constitui apenas na implantação de um novo pacote. O principal desafio é que envolve pessoas de culturas e propósitos diferentes, que idealmente devem ter os mesmos objetivos.

3.7.3. Centrais de Atendimento

As Centrais de Atendimento auxiliam de forma direta na implantação dos sistemas de CRM, sendo a ferramenta mais utilizada para sua implantação. Por este motivo são destacadas nesta tese, embora não representem, por si só, uma aplicação direta dos Sistemas de Informação.

Uma Central de Atendimento se constitui em um serviço da empresa, responsável pela interface com os clientes. Uma Central de Atendimento dispõe dos recursos computacionais que dão apoio aos Sistemas de Informação da empresa, disponibilizando aos atendentes toda a informação de que necessitem para realizar um atendimento de alto nível e com eficiência.

O principal canal de comunicação de uma Central de Atendimento é o telefone. No entanto, há ainda outros canais que podem ser utilizados, tais como a Internet e o Fax. Nem todas Centrais de Atendimento possuem esses outros canais de comunicação, sendo que a implantação desses recursos alternativos de atendimento deve ser analisada em cada empresa, avaliando-se seus custos e benefícios associados (SERRA, 2001).

A finalidade básica de uma Central de Atendimento é a de realizar o atendimento a clientes, existindo alguns objetivos paralelos. Dentre tais objetivos pode-se citar o de se estabelecer um canal de relacionamento com os clientes que possibilite sua identificação de forma personalizada, ao mesmo tempo em que estimule a fidelidade, valorizando a imagem da empresa.

As empresas estão implantando estratégias de tempo de atendimento limite dos chamados. Esse tempo pode ser por tipo de cliente ou contrato, por exemplo,

buscando um atendimento rápido e eficiente. Os especialistas que conseguem resolver os chamados no prazo estipulado podem ganhar bonificações ou prêmios por isso, o que estimula o desempenho nas chamadas.

As Centrais de Atendimento podem ser classificadas como sendo do tipo receptivo ou do tipo ativo (SERRA, 2001).

As Centrais de Atendimento receptivas recebem contatos de clientes e sua implantação mais comum recebe a denominação de *help desk*. As Centrais de Atendimento *help desk* são as que oferecem serviço especializado em um determinado produto ou serviço.

Geralmente, as pessoas que trabalham no *help desk* são especialistas e possuem um treinamento adequado para solucionar os problemas ou dúvidas do cliente no primeiro contato. Caso o especialista não consiga resolver o problema nesse primeiro contato, o chamado pode ser encaminhado para um estudo mais detalhado, para um analista de suporte ou ainda se efetuar um serviço remoto.

As Centrais de Atendimento ativas têm como objetivo a prospecção de clientes. Esse serviço na Central de Atendimento é conhecido como *telemarketing*, no qual o atendente entra em contato com possíveis clientes, visando divulgar ou oferecer produtos e serviços da empresa. A Central de Atendimento Ativa também pode ser utilizada para efetuar pesquisa de satisfação dos clientes, concluir chamados abertos ou para atualização e complementação de dados de clientes.

3.7.4. Gerência do Conhecimento

A Gerência do Conhecimento pode ser definida como o processo por meio do qual organizações conseguem gerar valor a partir do conhecimento adquirido por elas, seja esse conhecimento representado por dados propriamente ditos, seja por intermédio do conhecimento intelectual das pessoas componentes da organização. A Gerência do Conhecimento representa também a sistemática de pesquisa, coleta e organização do conhecimento em uma empresa (TURBAN; ARONSON, 1998).

Muitas das oportunidades que se colocam no atual mundo dos negócios se originam do conhecimento e informação, e não apenas da disponibilidade de ativos materiais.

Tal fato se constituí em uma das principais justificativas para que se façam investimentos na Gerência do Conhecimento.

O conhecimento pode ser dividido em duas categorias, que são o conhecimento explícito e o conhecimento tácito. O conhecimento explícito é representado por patentes, planos de negócio, pesquisas de marketing e listas de clientes, dentre outros. Dito de outra maneira, o conhecimento explícito pode ser documentado, arquivado e eventualmente codificado com o auxílio das Tecnologias da Informação. O conhecimento tácito é aquele contido na mente das pessoas, sendo que o problema é como reconhecer, capturar e gerenciar tal conhecimento.

O conhecimento explícito normalmente está organizado na forma de desenhos técnicos, manuais de processos, etc. O conhecimento tácito envolve o instinto, o discernimento e a experiência.

O principal desafio que se coloca é o de extrair o conhecimento tácito de funcionários, pois se estes não quiserem colaborar no processo, dificilmente se terá sucesso nessa tarefa. Uma das maneiras de se incentivar uma participação colaborativa é representada pela adoção de prêmios àqueles que colaborarem nessa prática. No entanto, a forma mais eficiente de obtenção do conhecimento tácito ocorre quando os funcionários se sentirem recompensados pela simples ação de fornecer informações aos sistemas de Gerência do Conhecimento.

A prática da Gerência do Conhecimento não é representada pela simples aplicação da tecnologia, mas deve estar inserida na filosofia geral da organização. A Gerência do Conhecimento não deve ser um elemento divorciado das metas globais da organização.

O conhecimento não é estático e, por isso mesmo, o conteúdo e as prioridades dos sistemas de Gerência do Conhecimento devem sofrer um processo contínuo de atualização.

Nem toda informação disponível em uma empresa representa um conhecimento útil para um sistema de Gerência do Conhecimento e portanto o processo de seleção das informações é extremamente importante na montagem dos sistemas para a Gerência do Conhecimento.

Algumas companhias têm um responsável exclusivamente dedicado ao acompanhamento dos sistemas de Gerência do Conhecimento, chamado de *Chief Knowledge Officer* (CKO). No entanto, tal função pode também ser assumida por outras pessoas da alta direção da empresa.

O compartilhamento do conhecimento é uma das maiores contribuições da Gerência do Conhecimento, pois difunde o mesmo pela organização, evitando a realização de pesquisas, estudos e trabalhos previamente realizados.

A Tecnologia da Informação tem o papel de ampliar o alcance e acelerar a velocidade da difusão do conhecimento. As ferramentas da Gerência do Conhecimento pretendem auxiliar no processo de captura e estruturação do conhecimento em uma base compartilhada a toda organização.

3.7.5. Sistemas de Gestão Empresarial

Sistemas de Gestão Empresarial, também conhecidos como Enterprise Resouce Planning – ERP, buscam integrar diversos setores de uma empresa, através da utilização de uma ferramenta de software, que conjugue diversos tipos de necessidades, tais como aplicações contábeis e controle de estoque, dentre outras.

Os sistemas de ERP entraram em uso no começo da década de 1990, tendo alguns predecessores, como o MRP – Material Resource Planning, MRPII – Manufacturing Resource Planning e CIM – Computer Integrated Manufacturing, todos apoiando a automação de diversos aspectos de uma empresa de manufatura. Simultaneamente, mas separadamente, foram desenvolvidos programas para apoiar transações contábeis e financeiras.

A integração dessa gama de ferramentas representa o conceito dos Sistemas de Gestão Empresarial, que, por ser uma ferramenta integrada, permite um trabalho também mais integrado, com os diversos setores de uma organização possibilitando o conhecimento das atividades como um todo (HAGMAN; GABLE, 2000).

Os principais benefícios advindos dessa integração são a agilização de transações financeiras, minimizando o tempo de confirmações de créditos e débitos, a obtenção de uma excelente base para o comércio eletrônico, além de tornar explícito o

conhecimento tácito, mapeando os principais processos, as regras de decisão e a estrutura de informação.

Uma das tendências notadas nos Sistemas de Gestão Empresarial é a de expansão de suas fronteiras, agregando ferramentas para o Gerenciamento da Cadeia de Suprimentos (SCM – Supply Chain Management) e até partes do CRM.

Uma das características do software desenvolvido para os sistemas ERP é que utilizam uma Base de Dados integrada e devem possuir alto potencial de personalização para cada empresa que o utilize. É possível utilizar os sistemas ERP em um ambiente globalizado, considerando-se diversas instalações físicas distribuídas geograficamente. O principal foco do processamento executado pelos Sistemas de Gestão Empresarial são as atividades executadas de forma repetitiva dentro das organizações.

Por ser um ambiente integrado, torna-se mais fácil a realização de alterações que se façam necessárias em um ambiente de negócios, que muitas vezes é bastante dinâmico.

3.7.6. Inteligência Empresarial

A Inteligência Empresarial, também conhecida como Business Intelligence, ou abreviadamente BI, consiste na habilidade em se obter conhecimento sobre uma empresa, através da utilização de técnicas automatizadas, disponibilizando-o a usuários em todos os níveis da empresa. Isto é vital a operações competitivas, permitindo que sejam tomadas decisões com a rapidez necessária (McLEOD, 1995).

Os sistemas de Inteligência Empresarial visam coordenar o modo de descrever todas as atividades de uma empresa ligadas ao gerenciamento, coleta, disseminação e exploração da inteligência. A inteligência pode ser definida como a capacidade de aprender, reter, processar e compreender ou de aplicar o conhecimento de forma a se poder manipular o seu ambiente.

A Inteligência Empresarial tem como objetivo a utilização dos dados de forma efetiva, os quais devem ser utilizados para otimizar os resultados de negócios das empresas. Outro objetivo é a geração de produtos, serviços e atendimento mais

adequados, maximizando a capacidade competitiva. A chave do sucesso dos negócios atuais está no fato de se conseguir acesso rápido e fácil à informação.

A principal fonte de dados utilizada pelos Sistemas de Inteligência Empresarial é composta pelo Data Warehouse, sendo que a forma básica de acesso são as ferramentas OLAP – OnLine Analytical Processing. Por meio de tais ferramentas, os próprios usuários são capazes de obter as informações de que necessitam, bem como na forma mais adequada.

A utilização de informações de forma inteligente é um dos requisitos para a sobrevivência no mundo dos negócios.

3.7.7. Comércio Eletrônico

O Comércio Eletrônico se constitui no uso da Tecnologia da Informação e redes de comunicação eletrônicas para troca de informações sobre negócios, conduzindo transações de forma eletrônica, ou seja, sem a utilização de formulários em papel. (HARMON et al., 2001).

O Comércio Eletrônico proporciona a realização de negócios sem barreiras físicas, seja dentro da própria empresa, seja entre empresas ou entre empresas e pessoas físicas. Daí surgem dois conceitos que são o B2B e o B2C. B2B significa *Business-to-Business* e indica a troca de informações entre organizações com o propósito de conduzir operações comerciais. B2C significa *Business-to-Consumer* e representa a realização de transações entre empresas e consumidores, onde são trocados valores por mercadorias ou por serviços.

O principal benefício do Comércio Eletrônico está na expansão das oportunidades de negócios, explorando o conceito de mercado globalizado, permitindo uma presença maior da empresa no mercado. Também se obtém uma melhora na comunicação, permitindo a divulgação dos produtos da empresa, bem como sua personalização a cada cliente, além de uma redução de custos, visto que transações feitas via Internet têm custo significativamente inferior quando comparadas às transações convencionais. O cliente também se beneficia pela possibilidade de maior

competição entre fornecedores, maior possibilidade de seleção de produtos e melhora do atendimento.

A partir do Comércio Eletrônico surgiram outros conceitos, como o *e-banking*, que é a Internet voltada para a realização de transações bancárias (MULUTINOVIC; PATRICELLI, 2002).

Outro conceito é o de *e-marketing*, cujas principais formas de atuação são a montagem de sites, visando a comunicação com os clientes, a colocação de faixas em outros sites ou a utilização de e-mail.

Nessa mesma linha, outro conceito utilizado é o Governo Eletrônico, que representa a possibilidade de cidadãos acessarem serviços governamentais sempre que necessário, a partir de qualquer localização.

Pode-se identificar quatro categorias de usuários do Governo Eletrônico que são: o próprio governo, permitindo a interoperabilidade entre agências governamentais; funcionários públicos, servindo como uma ferramenta de comunicação e consulta; empresas que busquem a obtenção de serviços, melhorando sua eficiência; e cidadãos na busca de informações, possibilidade de obtenção de licenças, certificados, pagamentos, etc.

3.7.8. Aplicações Multimídia

Neste tipo de aplicação, o foco está no processamento de imagens, áudio e vídeo. Uma característica importante é que os dados tratados neste tipo de aplicação são chamados de Dados de Meio Contínuo, o que significa que sons e vídeos devem ter os dados recuperados a taxas contínuas, de forma a não se verificar a ocorrência de perdas de continuidade na exibição das informações. Uma das técnicas utilizadas para corrigir tal problema constitui-se no emprego de *buffers*, desde que seja prevenida a ocorrência de *overflow* nos mesmos, de maneira a se evitar a perda de dados (SILBERSCHATZ et al., 2002).

As bibliotecas disponibilizadas pela Internet são um exemplo desse tipo de aplicação, contendo inúmeras publicações, informações em várias línguas, diversos formatos e volumes imensos de informação. Nesse tipo de aplicação, a organização tradicional

por autor, título e assunto não explora o potencial da computação na busca de informações, sendo que o desafio está no processo de encontrar informações relevantes em documentos, mapas, fotos, sons e vídeos.

Os documentos têm palavras chave, por meio das quais os usuários acessam ou realizam buscas nos assuntos de interesse. Nas consultas atribui-se um grau de relevância aos documentos localizados e também pode ser usada a busca por similaridade a um documento fornecido pelo usuário (base em palavras chave).

A indexação também é feita pelas palavras chave, sendo que a posição dessas palavras chave no texto é utilizada para que seja feita uma classificação da relevância de cada documento. Por exemplo, uma palavra chave localizada no resumo tem um valor muito maior do que uma palavra chave localizada no fim do documento.

Um exemplo de biblioteca multimídia é o WVTDB – *Web-Based Video Text Data Base System*, voltada para o ensino à distância. Suas características técnicas incluem a indexação pelas suas características visuais, tais como cor, formato, tipo de movimentação, áudio e conteúdo semântico (origem em anotações manuais e em *closed caption*) (JIANG; ELMAGRAMID, 1998).

Outro exemplo de Biblioteca Digital é o JSTOR - *Journal Storage*, da Universidade de Michigan. Nessa base de dados foi feita a conversão de periódicos antigos para formato digital, visando a preservação de seus conteúdos, bem como economia de espaço físico. Em fevereiro de 1999 havia 70 periódicos com 450.000 artigos e 2,7 milhões de páginas cadastradas nessa biblioteca digital. A taxa de crescimento apresentava um aumento de 100.000 páginas a cada mês (THOMAS et al., 1999).

Neste capítulo foram apresentadas as principais características de Sistemas de Informação, de forma a possibilitar, que no próximo capítulo, seja feito um estudo comparativo envolvendo os Sistemas de Informação e a sua Segurança de Informação, juntamente com os Sistemas Críticos e a sua Segurança Crítica, detalhados no capítulo 2.

4. ESTUDO COMPARATIVO DE SISTEMAS CRÍTICOS E DE SISTEMAS DE INFORMAÇÃO

As aplicações envolvendo Sistemas Críticos e Sistemas de Informação têm importância e utilidade enormes à sociedade atual. Praticamente não se concebe um mundo sem a existência de modernos Sistemas Críticos, comandando aplicações vitais, tais como sistemas de transporte público, indústrias químicas e siderúrgicas, bem como diversos equipamentos médicos, dentre outros.

Da mesma forma, é difícil de se imaginar como seria a vida nos dias de hoje sem os modernos Sistemas de Informação, representados por sistemas bancários, sistemas de reserva de passagens aéreas e todo o comércio eletrônico efetuado por meio da Internet. Apenas para citar alguns dados, em 1998, nos Estados Unidos, o custo de inatividade por hora, de alguns importantes sistemas computacionais estava estimado em:
US$ 1.150.000,00 para o sistema *pay-per-view* de operadoras de TV a cabo, US$ 2.600.000,00 para operadoras de cartões de crédito e US$ 6.500.000,00 para operadoras de bolsa de valores. Esses números consideram apenas as perdas diretas, não incluindo o efeito negativo do aspecto psicológico sobre a credibilidade das instituições envolvidas (IBM, 1999).

Por esses números pode-se perceber a enorme importância que tais sistemas computacionais representam, não apenas para as empresas operadoras desses sistemas, mas também no dia a dia dos cidadãos, considerando-se que a utilização de computadores já é um fato corriqueiro a grande parte da população.

Conforme já exposto no capítulo 2, com relação à Segurança Crítica, e no capítulo 3, com relação à Segurança de Informação, deve ser feita uma análise de segurança, ou ainda serem avaliados os riscos e seus impactos, de forma a se estabelecerem as medidas de proteção necessárias a cada sistema.

A partir dessas avaliações, decidem-se as medidas a serem tomadas, como, por exemplo, refazer o projeto ou partes dele, acrescentar elementos para tentar garantir a segurança, ou ainda considerar que se possa conviver com uma probabilidade muito baixa de ocorrência de eventos perigosos.

Ao lado da propriedade da Segurança Crítica ou da Segurança de Informação, a propriedade da disponibilidade também representa um aspecto fundamental. Quando se projetar a disponibilidade necessária a um sistema computacional, deve-se atribuir prioridades a cada uma das partes e funcionalidades dos sistemas, de tal forma que os pontos críticos possam apresentar a maior disponibilidade possível, ou seja, estarem disponíveis quando de fato tiverem maior probabilidade de serem acessados.

Dando continuidade e este estudo comparativo, realiza-se, no próximo item, uma comparação dos principais aspectos envolvidos tanto em Sistemas Críticos, quanto em Sistemas de Informação.

4.1. Comparação entre Sistemas Críticos e Sistemas de Informação

Neste item é feita a comparação de cada um dos aspectos abordados nos capítulos 2 e 3, voltados a Sistemas Críticos e a Sistemas de Informação, respectivamente.

Em uma Aplicação Crítica quase sempre há associada alguma ação física, como por exemplo, a ação de ligar ou desligar um motor, o acionamento de freios, a emissão de uma determinada quantidade de raios X, e assim por diante. Neste caso, os riscos estão relacionados à probabilidade de ocorrência de acidentes, tais como a queda de um avião ou um choque entre dois trens.

Em uma Aplicação de Sistemas de Informação, pode-se dividir os riscos existentes em duas categorias, que são a manutenção da consistência e da integridade de dados e a prevenção contra invasões de sistemas, por pessoas ou sistemas não autorizados.

Na primeira categoria, representada pela manutenção da consistência e da integridade de dados de um sistema, as principais ameaças que põem em risco esse objetivo são compostas por falhas em seus componentes de hardware, módulos do software, ou ainda fatores externos, tais como interferências eletromagnéticas. Na segunda categoria, representada pela prevenção contra invasões do sistema, as principais ameaças são compostas por pessoas que tenham interesse em furtar informações sigilosas ou confidenciais que não lhes pertençam. Há intersecções entre essas duas categorias de riscos em Sistemas de Informação, como por exemplo, um invasor alterando propositalmente os dados, fazendo com que percam sua consistência.

Diferente das Aplicações Críticas, um Sistema de Informação não tem associada a si ações físicas, mas apenas ações eletrônicas, representadas pelo armazenamento e recuperação de informações.

Antes de se fazer as comparações propriamente ditas, convém destacar a necessidade de se criar uma denominação que abranja os dois tipos de sistemas e os dois tipos de segurança. Para a junção dos Sistemas Críticos e Sistemas de Informação, será adotada a denominação Sistemas Computacionais de Segurança e para a junção da Segurança Crítica e Segurança de Informação será adotada a denominação Segurança Computacional. Por junção está se querendo dizer que tanto os Sistemas Críticos irão herdar as principais características dos Sistemas de Informação, quanto os Sistemas de Informação irão absorver as características básicas dos Sistemas Críticos. Pode-se dizer o mesmo com relação à Segurança Crítica e à Segurança de Informação.

4.1.1. Comparação da Segurança Crítica e Segurança de Informação

Há diversos fatores a serem comparados no que diz respeito à Segurança Crítica e à Segurança de Informação. A começar pela comparação da definição dos dois conceitos. Por Segurança Crítica entende-se a probabilidade de que, em um determinado período de tempo, o sistema não atinja um estado considerado inseguro, a partir do qual possam vir a ocorrer acidentes. Por Segurança de Informação entende-se a proteção de informações e de seu respectivo sistema computacional contra processamento não autorizado, erros e incidentes. Uma aproximação entre os conceitos de Segurança Crítica e Segurança de Informação irá ocorrer se, em um Sistema de Informação, a perda e a consulta não autorizadas de informações forem consideradas situações perigosas.

Há uma tendência, que também aponta para o sentido de fusão de conceitos, de que a Segurança de Informação possa a ser encarada como um pré-requisito para a Segurança Crítica, ou seja, se não houver Segurança de Informação, também não haverá garantia da manutenção da Segurança Crítica.

Outro fator comum está no problema da ocorrência de atos maliciosos, que podem vir a ocorrer nos Sistemas Críticos e nos Sistemas de Informação. Portanto, deve haver a prevenção contra as suas conseqüências, considerando-se os dois tipos de aplicações, ou ainda a sua junção.

Conforme destacado no capítulo 2, os três conceitos básicos envolvidos na Segurança Crítica são, além da segurança em si, a confiabilidade, a disponibilidade e a mantenabilidade. No capítulo 3, os três pontos básicos destacados na Segurança de Informação são a disponibilidade, a confidencialidade e a integridade dos dados, além da segurança propriamente dita.

Pode-se verificar que um dos fatores em comum aos dois tipos de segurança é a disponibilidade dos sistemas. Em ambos os casos, há a necessidade de que os sistemas operem de forma contínua, sem interrupções. No caso da Segurança Crítica, uma baixa disponibilidade representa que uma aplicação importante está indisponível, deixando de proporcionar os benefícios associados, tais como geração de energia ou a operação de um sistema de transporte, podendo ocasionar acidentes e perda de credibilidade do respectivo serviço. No caso da Segurança da Informação, a não disponibilidade de um sistema representa que um serviço, normalmente de grande interesse e importância, não pode ser acessado, podendo gerar perdas econômicas e de credibilidade.

Por esta análise pode-se notar a existência de um aspecto comum que ocorre no caso de uma baixa disponibilidade de Sistemas Críticos e de Sistemas de Informação, que é o problema da credibilidade dos mesmos junto à população. A credibilidade e confiança são difíceis de conquistar, porém muito fáceis de serem perdidas.

O fator da confiabilidade, citado no caso da Segurança Crítica, pode ser comparado com o fator de integridade de dados, da Segurança de Informação. A confiabilidade representa a probabilidade de um sistema permanecer sem falhas por um período de tempo, considerando que, no instante inicial, o mesmo encontrava-se funcionando corretamente, enquanto que a integridade de dados representa a propriedade dos dados continuarem a ter seus valores dentro de faixas consideradas como válidas. Embora suas definições sejam diferentes, o sentido é semelhante, indicando a

necessidade de que usuários possam manter a confiança nos sistemas que estiverem utilizando.

No caso da Segurança Crítica, a confidencialidade dos dados não tem a mesma importância que no caso da Segurança de Informação, tendo em vista que, em sua grande maioria, as Aplicações Críticas são sistemas fechados, não possibilitando invasões por parte de usuários não autorizados. No entanto, há uma tendência de se efetuar a supervisão e controle de Sistemas Críticos também por meio de redes de comunicação de dados, e até pela Internet. Nesse caso, torna-se necessário, também nos Sistemas Críticos, ter a preocupação com a confidencialidade e com a segurança de dados recebidos e enviados às Aplicações Críticas.

Já no caso da mantenabilidade, sua importância é grande em ambos os tipos de segurança, pelos mesmos fatores apontados no caso da disponibilidade.

Portanto, pela análise comparativa desses dois conjuntos de propriedades da Segurança Crítica e da Segurança de Informação, pode-se observar que há grandes analogias entre ambos, permitindo reunir, gradativamente, os conceitos na Segurança Computacional.

Comparando-se o aspecto de conseqüências de falhas, tanto nos Sistemas de Informação, quanto nos Sistemas Críticos, nem todas as falhas existentes resultam em estados perigosos, em acessos não autorizados ou em acidentes. Apenas uma pequena parcela dessas falhas é que pode, de fato, representar situações não desejadas às aplicações. Mais uma vez observa-se a analogia entre os dois tipos de aplicação, permitindo-se supor uma fusão incremental dos conceitos de segurança.

Finalmente, outra confrontação que produz resultado semelhante, está na necessidade de se verificar quais são, de fato, as partes de um sistema ou porções de informação que devem ser protegidas, o que se constitui em outra característica comum aos dois tipos de segurança. Ou seja, o objetivo desta verificação é o de concentrar esforços para a manutenção da segurança nos setores mais importantes ou mais vulneráveis dos sistemas. Mais uma vez, pode-se dizer que há uma tendência de reunião dos dois conceitos de segurança.

De uma forma geral, pelas comparações feitas neste item, pode-se afirmar que é viável uma fusão gradual dos dois conceitos de segurança, na chamada Segurança Computacional.

4.1.2. Comparação da Cultura de Segurança

Comparando-se a cultura estabelecida para Sistemas Críticos e para Sistemas de Informação, pode-se verificar a existência de um fator de diferenciação. Nos Sistemas Críticos, a maior preocupação é com falhas do próprio sistema, enquanto que em Sistemas de Informação, a maior preocupação está em atos maliciosos representados por invasões aos sistemas. No entanto, conforme já estabelecido no item anterior, na comparação da Segurança Crítica e da Segurança de Informação, pode-se afirmar que há uma tendência de se efetuar a supervisão e controle de Sistemas Críticos também por meio de redes de comunicação de dados, e até pela Internet. Neste caso, as invasões também passarão a representar um grande fator de preocupação nos Sistemas Críticos. Desta forma, com relação a este aspecto, a Cultura de Segurança vem aos poucos se tornando semelhante.

Sem uma cultura global de segurança não é possível a manutenção da segurança de nenhum sistema, seja crítico, seja de informação. Portanto é necessário que haja a conscientização de todos os envolvidos na operação dos dois tipos de sistemas, Críticos ou de Informação.

Um aspecto de grande importância tanto na Cultura de Segurança Crítica, quanto na Cultura de Segurança de Informação é o treinamento sobre o sistema. Um treinamento eficaz se constitui em um dos aspectos primordiais a serem observados, tendo influência na maneira como o sistema é utilizado e na cultura geral sobre a segurança. Desta forma, pode-se pensar em uma fusão parcial dos dois conceitos, chegando-se na Cultura de Segurança Computacional.

Outro ponto a ser observado em qualquer sistema em que a segurança seja um fator importante é o envolvimento da alta direção das organizações. Realizando-se uma comparação entre os dois tipos de cultura, esse envolvimento é necessário em ambos, não apenas pelo fator econômico da liberação de recursos destinados à manutenção

da segurança em geral, mas também pelo incentivo que a direção deve proporcionar a todos os funcionários, no sentido de sempre zelarem pela segurança de seus sistemas. Mais uma vez, observa-se a possibilidade de fusão dos dois conceitos de Cultura de Segurança.

Também deve ser encarado como um fator de grande importância, a existência e a conseqüente divulgação da política de segurança adotada pela empresa. Essa política de segurança deve abranger todos os pontos identificados como críticos, de forma a cobrir todas as ameaças e perigos potenciais aos sistemas. Uma ampla divulgação é necessária para que todos estejam conscientes da forma de agir, no caso da ocorrência de qualquer tipo de problema relativo à segurança, seja a Segurança Crítica, seja a Segurança de Informação. Também é importante que a política de segurança seja flexível, permitindo adaptações, conforme as condições perigosas forem se modificando. Portanto, confrontando-se este aspecto da política de segurança, verifica-se a viabilidade de reunião dos dois conceitos de Cultura de Segurança.

Finalmente, na comparação da importância da tecnologia empregada nos sistemas, deve-se estar consciente de que a mesma é importante, ou seja, sem a tecnologia não existiriam muitas das formas de proteção atualmente utilizadas. No entanto, talvez mais importante que os aspectos tecnológicos, há a necessidade de que todos na organização mantenham uma preocupação constante com o aspecto segurança. Apenas com a junção da tecnologia com a vigilância permanente de funcionários, é que se pode ter sucesso em um plano de garantia da segurança, sendo que esta conclusão é válida nas duas categorias de Cultura de Segurança.

Mais uma vez, tendo em vista os confrontos realizados neste item, é possível se concluir que a fusão dos conceitos de Cultura de Segurança é factível, podendo ocorrer de forma incremental, resultando no conceito único denominado de Cultura de Segurança Computacional.

4.1.3. Comparação dos Requisitos de Segurança

Confrontando-se os Sistemas Críticos e os Sistemas de Informação, o objetivo principal para o estabelecimento de seus Requisitos de Segurança é o de evitar as condições perigosas ou vulneráveis, prevenir a ocorrência de acidentes ou de invasões que possam vir a ocorrer em função dessas condições perigosas, e finalmente minimizar as conseqüências advindas em função de um eventual acidente ou invasão. Para que isso seja possível, é necessário que se identifiquem todas as condições perigosas que possam vir a ocorrer, classificar tais condições dentro de uma escala de prioridades e determinar os métodos mais apropriados para o tratamento dessas condições. Portanto, sob o ponto de vista do estabelecimento dos Requisitos de Segurança, ambos os tipos de sistemas apresentam muitas similaridades, apontando para a possibilidade de fusão nos Requisitos de Segurança Computacional.

Efetuando-se uma comparação entre os requisitos estabelecidos para Sistemas Críticos e Sistemas de Informação, pode-se dizer que há diversos requisitos gerais com praticamente a mesma relevância a esses sistemas. Dentre tais requisitos destacam-se o desempenho, a disponibilidade, a confiabilidade, a usabilidade e uma documentação completa. A identificação de riscos e de ameaças aos sistemas também é um fator comum aos dois tipos de aplicação. Portanto, no que tange aos requisitos gerais, pode-se pensar no estabelecimento de Requisitos de Segurança Computacional.

Dentre os requisitos gerais de ambas as categorias de sistemas, devem ser destacados aqueles referentes à manutenção dos sistemas, tendo em vista que tal propriedade é de suma importância, pois de nada adianta ter uma série de redundâncias implementadas, se na ocorrência de falhas, o sistema não for recomposto ao seu estado original, sem falhas. Assim por exemplo, deve ser especificado o Tempo Médio para Reparo do sistema.

Os requisitos gerais devem sofrer um processo de detalhamento, à medida que as arquiteturas dos sistemas vão sendo projetadas, resultando nos Requisitos Específicos de Segurança. Estes requisitos, particulares a cada implementação,

também possuem diversos aspectos comuns. Por exemplo, seja qual for a aplicação, devem ser estabelecidos requisitos qualitativos, referentes a propriedades não quantificáveis dos sistemas, tais como qualidade, testabilidade, legibilidade do código, dentre outros. Requisitos quantitativos também devem ser previstos, tais como o Tempo Médio entre Falhas e o desempenho dos sistemas. Uma comparação entre os Requisitos de Segurança Específicos dos dois tipos de sistemas permite novamente reafirmar a possibilidade de sua fusão, resultando nos Requisitos de Segurança Computacional.

Há ainda, uma série de requisitos implícitos que devem ser contemplados por projetos, supostamente, bem elaborados, como por exemplo, facilidade de manutenção e de realização de testes. Estes requisitos são inerentes aos dois tipos de sistemas, críticos e de informação.

Considerando-se as comparações aqui realizadas, é possível se concluir que pode ser feita, parcial e gradativamente, a fusão dos conceitos relativos aos Requisitos de Segurança, resultando no conceito único denominado de Requisitos de Segurança Computacional.

4.1.4. Comparação da Implementação

Comparando-se o aspecto da implementação de Sistemas Críticos e de Sistemas de Informação, há pelo menos dois fatores que os afetam de forma semelhante. Em primeiro lugar vem a confiabilidade dos componentes utilizados, bem como dos circuitos integrantes do hardware utilizado. O segundo aspecto refere-se à capacidade de detecção de falhas, a qual deve funcionar da maneira mais rápida possível, indicando também a localização de falhas e até de ações corretivas, ou ainda realizando reconfigurações dinâmicas do sistema.

Outro ponto a se comparar e considerar é que, na detecção de uma falha, deve-se procurar fazer seu isolamento, prevenindo-se a sua propagação a outras partes ou a todo o sistema. As medidas de restauração de um sistema a seu funcionamento normal, após a ocorrência e detecção de uma falha são, em ambos tipos de aplicações: a recuperação do serviço por meio de elementos redundantes presentes no

sistema, a substituição ou a restauração do elemento com falha, que pode envolver também a utilização de arquivos de histórico de transações efetuadas e a reintegração do elemento já restaurado ou eventualmente substituído.

Sob esses três aspectos descritos, os dois tipos de sistemas abrangem os mesmos conceitos, permitindo que se pense na possibilidade do conceito de Implementação de Sistemas Computacionais.

Realizando-se o confronto entre Sistemas Críticos e Sistemas de Informação, a questão da implementação de um sistema onde a segurança esteja envolvida, depende, principalmente, de sua qualidade de projeto. A qualidade exigida em computadores que exercem funções de segurança deve ser atingida tanto pelo hardware, como pelo software que compõem o sistema em questão, considerando-se ambos os tipos de sistemas.

Tanto nos Sistemas Críticos, quanto nos Sistemas de Informação, as especificações são o ponto de partida para a realização das atividades de desenvolvimento de seus produtos. As especificações são escritas a partir de requisitos estabelecidos pelo cliente, e seu conteúdo final deve ser determinado de comum acordo por este último e pelos projetistas.

Quando da elaboração das especificações de um sistema, devem ser definidas todas as grandes funções de uma forma encadeada e não ambígua. Todas as interfaces entre os elementos do sistema devem ser definidas, bem como estabelecidos níveis de exigência de desempenho para o sistema. Na especificação devem ser separados os aspectos funcionais, das questões da implementação propriamente dita. A especificação é uma descrição daquilo que é desejado e não de como deve ocorrer sua implementação. Portanto, comparando-se os Sistemas Críticos e os Sistemas de Informação, ambos necessitam de especificações corretamente elaboradas, que irão servir de base para o desenvolvimento dos sistemas.

De forma a se realizar uma avaliação mais aprofundada, nos próximos dois itens são descritas as comparações realizadas entre as implementações de hardware e de software de Sistemas Críticos e Sistemas de Informação.

4.1.4.1. Comparação do Hardware

Tanto os Sistemas Críticos, quanto os Sistemas de Informação, devem ter seu processamento feito em sistemas computacionais que apresentem redundâncias em seus diversos componentes de hardware. Desta forma, os principais componentes que devem apresentar redundâncias são os processadores, memórias, discos rígidos, barramentos, sensores de entrada e atuadores de saída. Sem a implementação de módulos redundantes, não é possível a manutenção dos níveis de segurança, confiabilidade e disponibilidade exigidos para a maioria dos Sistemas Críticos e Sistemas de Informação.

Assim como a redundância é importante, também é fundamental, nos dois tipos de sistemas, a utilização de componentes confiáveis, ou seja, se houver componentes com menores taxas médias de falhas, estes devem ser utilizados, mesmo considerando-se que seu custo de aquisição seja superior ao de componentes com maiores taxas médias de falhas.

Nessa mesma linha de raciocínio, enquadra-se a utilização de componentes de última geração. Normalmente tais tipos de componentes costumam apresentar comportamento não totalmente previsível, tendo em vista não possuírem, ainda, um histórico de utilização e de ocorrência de falhas, amplo o suficiente, para que possam ser convenientemente avaliados. Sendo assim, para ambos os tipos de sistemas, não se recomenda a utilização deste tipo de componentes, embora os mesmos tenham grande utilização em Sistemas de Informação.

Outro ponto em comum pode ser observado na comparação entre mecanismos de detecção e recuperação de falhas, que são necessários em ambos os tipos de sistemas. Tal fato se justifica porque não há sentido em se ter toda uma estrutura de redundância implementada, se não se souber que determinado módulo possa ter apresentado falha, disparando o processo de substituição ou reconfiguração do sistema. Portanto, os Sistemas Críticos e os Sistemas de Informação devem possuir eficientes mecanismos de detecção e recuperação de falhas.

Um fator de diferenciação está no fato de que em Sistemas Críticos, praticamente todos os circuitos utilizados são especialmente desenvolvidos para esse tipo de utilização. Já em Sistemas de Informação é bastante comum o uso de placas e circuitos de propósito geral, cujos cuidados no projeto, desenvolvimento e montagem não são os mesmos exigidos para os Sistemas Críticos.

Em Sistemas Críticos, é comum a existência de um módulo comparador ou votador na saída dos sinais, implementado de acordo com a técnica de falha segura, de forma que qualquer falha nesse circuito leve o sistema a um estado sabidamente seguro. Normalmente, esse módulo, projetado de acordo com a técnica de falha segura, era implementado por circuitos discretos, tendo em vista que não se consegue implementar circuitos do tipo falha segura com a utilização de processadores. Mesmo esse paradigma tem sofrido alterações, já se encontrando circuitos de comparação ou de votação implementados por intermédio de circuitos com processadores, aproximando mais as implementações.

Outro aspecto comum que se observa na confrontação dos dois tipos de sistemas está na necessidade de modelagem da arquitetura projetada para o hardware, de forma a que se obtenham valores de suas taxas médias de falhas, permitindo avaliar se a utilização de determinado circuito pode ou não ser feita, considerando-se os parâmetros determinados em sua especificação. Para o cálculo desses valores das arquiteturas de hardware, normalmente se utilizam as formas de modelagem por Redes de Petri, Métodos de Markov e Statecharts.

Finalmente, tanto as Aplicações Críticas, quanto os Sistemas de Informação devem possuir planos de contingência e de recuperação de desastres, sempre visando a manutenção da disponibilidade das aplicações.

Considerando-se as comparações aqui realizadas, é possível se concluir que pode ser feita, gradual e parcialmente, a fusão dos conceitos relativos ao hardware de Sistemas Críticos e de Sistemas de Informação, vindo a resultar no conceito único denominado de Hardware de Segurança Computacional. Conforme já apontado, o principal fator que impede uma aproximação mais abrangente está no cuidado prestado ao projeto dos circuitos.

4.1.4.2. Comparação do Software

O hardware é reproduzido em grandes quantidades (em geral, muito maiores que o software), utilizando componentes já conhecidos. A confiabilidade pode ser medida e melhorada com base em informações colhidas na análise de projetos anteriores. O software, por outro lado, é quase sempre feito especialmente para cada aplicação, o que dificulta a comparação com outras aplicações. Isto ocorre principalmente para o software de Sistemas Críticos.

Um fator comum aos dois tipos de sistemas está nas especificações. A principal causa da presença de falhas no software, seja em Sistemas Críticos, seja em Sistemas de Informação, são as falhas cometidas na especificação. Os testes podem mostrar que existe aderência de um programa às especificações, mas não podem, no entanto, identificar erros eventualmente presentes em tais requisitos. Estes são apenas percebidos através da utilização do sistema no ambiente real para o qual foi projetado (HOFMANN, 2001).

Desta forma, considerando-se Sistemas Críticos e Sistemas de Informação, as especificações têm um papel central no desenvolvimento de software, pois devem definir todas as características requeridas de um programa a ser implementado, formando o ponto de partida de qualquer processo de desenvolvimento de um software. As especificações são também um importante meio de comunicação entre o cliente e o projetista, podendo até desempenhar o papel de um contrato formal, que pode ser utilizado para se verificar se o sistema implementado corresponde ao que foi solicitado.

Em Sistemas de Informação faz-se uso freqüente de Sistemas Operacionais, Sistemas Gerenciadores de Bases de Dados e de uma série de outras ferramentas comercialmente utilizadas. Tais ferramentas não possuem, em quase a sua totalidade, nenhum tipo de certificação de segurança, e por isso mesmo, raramente são utilizadas em Sistemas Críticos. Nestes últimos, praticamente não há a utilização dessas ferramentas, e toda programação é feita a cada sistema em particular. Pode-se dizer que as únicas ferramentas comerciais utilizadas são os compiladores, e mesmo nesse caso, recomenda-se uma série de precauções em seu uso.

Outro fator de diferenciação está nos cuidados de desenvolvimento, que são muito maiores para o software de Sistemas Críticos, em comparação com o software de Sistemas de Informação, refletindo-se até na forma de Análise de Segurança, conforme comentado no próximo item.

Uma constatação válida para os Sistemas Críticos e os Sistemas de Informação refere-se ao nível de organização e de maturidade da instituição, que exerce grande influência no software produzido, podendo-se afirmar que quanto maior a maturidade da empresa no desenvolvimento de programas com essa finalidade, melhores e mais seguros serão os novos programas produzidos.

Considerando-se as comparações aqui realizadas, chega-se à conclusão de que a maioria dos pontos considerados é divergente no que se refere ao desenvolvimento de software para Sistemas Críticos e para Sistemas de Informação. Para que seja possível a adoção, mesmo que gradual, de um conceito único, aqui denominado de Software de Segurança Computacional, há a necessidade de uma maior aproximação entre as formas de desenvolvimento atualmente utilizadas.

4.1.5. Comparação dos Métodos de Análise de Segurança

Comparando-se os métodos de Análise de Segurança para Sistemas Críticos e para Sistemas de Informação, percebe-se que há distinções entre eles. Nos Sistemas Críticos a atenção se volta para a busca de situações, seja em funcionamento, normal, seja na ocorrência de falhas, que possam levar o sistema a um possível estado perigoso. Tais estados perigosos concentram-se em situações que possam levar a aplicação controlada pelo Sistema Crítico a possíveis acidentes.

No caso dos Sistemas de Informação, a análise é direcionada à descoberta de situações que possam, quebrar a consistência dos dados, bem como possibilitar a ocorrência de invasões, permitindo o furto de informações ou mesmo a sua adulteração intencional.

Em ambos os casos, as condições não desejadas podem se originar a partir de falhas no hardware, no software ou de procedimentos operacionais. A partir da identificação de condições perigosas ou de ameaças potenciais aos sistemas, busca-se

verificar se existem mecanismos que possam combater tais condições, de forma a bloquear, por antecipação, a ação desses eventos.

Em ambos os casos é necessária a realização de testes funcionais e de testes de desempenho, de forma a se verificar se as especificações estão sendo cumpridas. Também é necessário que se faça uma análise dos parâmetros de qualidade e quantidade estabelecidos nas especificações de forma a se verificar ou não o seu cumprimento.

Considerando-se as comparações aqui realizadas, chega-se à conclusão de que há diversos aspectos distintos entre a Análise de Segurança realizada em Sistemas Críticos e em Sistemas de Informação, embora haja algumas etapas em comum. Se o número de etapas comuns vier a crescer, a Análise de Segurança dos dois tipos de sistemas poderia vir a ser reunida sob o conceito de Análise de Segurança Computacional.

4.1.6. Comparação das Normas

Comparando-se as normas voltadas a Sistemas Críticos e aquelas voltadas a Sistemas de Informação, verifica-se que há uma diferença de enfoque entre elas. As normas voltadas a Sistemas Críticos têm a preocupação principal na garantia de que o sistema não atinja estados considerados como inseguros. Se tal fato ocorrer, deve-se procurar sair o mais rapidamente possível desses estados, buscando-se estados considerados seguros, evitando-se a ocorrência de condições que propiciem a ocorrência de acidentes. Já as normas voltadas a Sistemas de Informação têm como preocupações principais a garantia da disponibilidade, sigilo e integridade das informações.

Se forem conjugados ambos os conceitos, considerando-se que um Sistema de Informação também seja Crítico, tendo em vista a severidade das conseqüências provocadas por falhas ou invasões, as normas da área crítica também passarão a ser aplicadas aos Sistemas de Informação. Se isto ocorrer, a tendência é que, em um futuro não muito distante, deixem de existir normas específicas a cada área, passando a existir um conjunto único de normas que satisfaça aos dois tipos de aplicações.

Se, por outro lado, for mantida a diferenciação de conceitos entre Sistemas Críticos e Sistemas de Informação, pode-se dizer que continuarão a co-existir normas voltadas a Sistemas de Informação e normas voltadas a Sistemas Críticos, embora muitos dos conceitos de cada área possam vir a ser aproveitados na outra área.

Vale destacar que as populações de seus respectivos países também desempenham papel importante na proposição dessas normas, tendo em vista que, quanto maior o grau de conscientização dos indivíduos, mais exigentes serão as condições estabelecidas, e por conseqüência melhores as condições de segurança exigidas, seja em Sistemas Críticos, seja em Sistemas de Informação.

Tendo em vista as comparações aqui realizadas, chega-se à conclusão de o aspecto que causa a distinção entre as normas voltadas às duas áreas está na diferenciação de conceitos atualmente existente. Se os conceitos relativos aos Sistemas de Informação forem revistos, no aspecto relativo à severidade das conseqüências provocadas por falhas ou invasões, pode-se pensar em futuras normas voltadas a Sistemas Computacionais de Segurança e sua Segurança Computacional.

4.1.7. Comparação das Aplicações

Nas aplicações descritas nos capítulos 2 e 3 há uma grande diferença no que se refere aos tipos de Aplicações Críticas e Sistemas de Informação.

Em todas as Aplicações Críticas há o envolvimento de alguma ação física associada, conforme descrito no item 4.1. Assim, na geração nuclear de energia, por exemplo, há uma série de ações físicas associadas, desde a própria reação nuclear, até a geração de energia propriamente dita. Situações similares ocorrem nas demais aplicações.

Nos Sistemas de Informação não há ações físicas diretamente associadas à sua operação, ou seja, a aplicação é computacional. Em todas as aplicações descritas há o uso intensivo de bases de dados e de ferramentas de software utilizadas para o processamento desses dados.

O uso de bases de dados, fundamentais em Sistemas de Informação, é ainda restrito em Aplicações Críticas, tendo em vista que o volume de dados, normalmente

necessário, não é muito grande. Pode-se dizer que há uma tendência de aumento da quantidade de dados necessários e utilizados em Aplicações Críticas.

Um fator comum a todas as aplicações é a necessidade de grande disponibilidade dos sistemas. No caso de Aplicações Críticas, a indisponibilidade de seu Sistema Crítico pode significar grandes transtornos à população, como a não geração de energia, o cancelamento de vôos, a paralisação de produção de indústrias em geral, ou o que é mais sério, a ocorrência de acidentes.

No caso de Sistemas de Informação, a sua indisponibilidade pode significar grandes perdas econômicas e de credibilidade das empresas, como por exemplo, sistemas de instituições financeiras, sistemas de centrais de atendimento, e assim por diante.

Como exemplo de aplicação comum, pode-se citar o desenvolvimento do conceito de redes de comunicação com a propriedade da Segurança Crítica. Tais redes estão em estudo e em testes preliminares, demonstrando a viabilidade desse conceito (MONTAGUE, 2002). Os principais aspectos envolvidos são a detecção de falhas, reconfiguração de rede e existência de redundâncias.

Uma possível unificação dos dois tipos de aplicação somente será adotada se for considerado que ambos, Sistemas de Informação e Aplicações Críticas tenham conseqüências similares em caso de disfunções, resultando nas Aplicações Computacionais de Segurança. Pode-se afirmar que esta tendência vem ocorrendo de forma gradual e incremental.

4.2. Escopo de Aplicações Críticas e Sistemas de Informação

Neste item faz-se uma avaliação do escopo de Aplicações Críticas e de Sistemas de Informação, tendo em vista a comparação já iniciada no item anterior.

Desta forma, nos próximos itens são apresentadas diversas opiniões encontradas na literatura, favoráveis ou não à fusão dos conceitos de Aplicações Críticas e Sistemas de Informação, bem como de Segurança de Informação e Segurança Crítica. Após a exposição de cada comentário encontrado na literatura, coloca-se a opinião do autor a respeito do respectivo item.

4.2.1. Conceitos de Segurança Crítica e Segurança de Informação

Segundo Leveson e Heimdahl (1998), a Segurança Crítica e a Segurança de Informação possuem muitas similaridades. A primeira delas é que ambas lidam com ameaças ou com riscos. A Segurança Crítica se preocupa, em primeiro lugar, com ameaças à vida ou propriedade, enquanto que a Segurança de Informação tradicionalmente se preocupa com a privacidade e com a segurança nacional. Devido ao interesse e à importância cada vez maior da informação em nossa sociedade, essa diferença vem diminuindo e até desaparecendo.

Ambos os tipos de Segurança envolvem características negativas, no sentido de impor restrições ao funcionamento de sistemas, que podem acabar por gerar conflitos entre funcionalidades importantes. A Segurança Crítica e a Segurança de Informação envolvem proteção contra perdas, embora os tipos de perdas envolvidos sejam de natureza distinta.

Uma distinção feita por Leveson e Heimdahl (1998) é que a Segurança de Informação está diretamente ligada a ações maliciosas, enquanto que a Segurança Crítica não está relacionada com ações dessa natureza, mas apenas com falhas dos sistemas.

De uma forma geral, a opinião de Leveson e Heimdahl (1998) coincide com a opinião do autor de que está havendo uma aproximação gradativa entre os Sistemas Críticos e os Sistemas de Informação. O aspecto destoante é que os dois autores apontam a ocorrência de atos maliciosos apenas contra Sistemas de Informação, o que nem sempre é verdade, pois estes também podem ser praticados contra Sistemas Críticos.

Outro trabalho que questiona o problema da junção dos conceitos de Segurança Crítica e Segurança de Informação é o artigo de Eames e Moffett (1999). No artigo, coloca-se a questão de que os sistemas de supervisão e controle computadorizados vêm tendo uma participação crescente em áreas aonde uma falha possa ter sérias conseqüências.

Dentro de cada um de seus domínios foram desenvolvidas técnicas especializadas para a geração de especificações de requisitos. Contudo, os sistemas mais recentemente projetados e colocados em uso, têm apresentado, freqüentemente, a necessidade de satisfazer as propriedades da Segurança Crítica e da Segurança de Informação, de forma simultânea. Tal fato vem fazendo com que o interesse em se pesquisar técnicas de desenvolvimento que atendam simultaneamente às propriedades da Segurança Crítica e da Segurança de Informação venha crescendo de forma bastante acentuada.

Tanto a Segurança Crítica, quanto a Segurança de Informação envolvem o tratamento de riscos, assim como ambas categorias de segurança estabelecem os requisitos de forma restritiva ou negativa, como por exemplo, um sistema não pode ter esse ou aquele comportamento. Ambos tipos de segurança envolvem a adoção de medidas de proteção contra os riscos previamente identificados. Tais similaridades podem indicar que algumas das técnicas utilizadas em um dos domínios podem ser utilizadas no outro domínio.

No entanto, de acordo com Eames e Moffett (1999), parece um tanto quanto inapropriado tentar unificar as técnicas de análise de risco de Segurança Crítica e de Segurança da Informação. A união dos dois tipos de análise pode levar projetistas a reduzir seu grau de conhecimento sobre o sistema em análise. Tentativas de unificar as duas técnicas podem envolver compromissos de ambos os lados, havendo a possibilidade de se obter uma análise incompleta, deixando de lado aspectos importantes da Segurança Crítica e da Segurança de Informação. Um risco adicional da junção das duas técnicas de análise é o de esconder os conflitos entre os requisitos, que muitas vezes auxiliam na resolução de problemas. Freqüentemente esse processo de solucionar conflitos se constitui, por si só, na forma mais proveitosa de se compreender o sistema.

Na análise de Eames e Moffett (1999) há vantagem em se integrar os conceitos de Segurança Crítica e Segurança da Informação, mas não de unificá-los. Desta forma, pode-se pensar em cada um desses domínios de forma coordenada, harmonizando-se as técnicas de cada um desses domínios. Tal aproximação tem o objetivo de tirar

proveito das vantagens de cada domínio, sem se perder o foco específico de cada um deles.

Ainda segundo Eames e Moffett, as técnicas específicas desenvolvidas para a Segurança Crítica e para a Segurança de Informação não seriam perdidas ou compromissadas. Conflitos tornam-se mais aparentes com as técnicas sendo aplicadas de forma isolada, porém coordenada, tornando possível a realização de comparações. O cruzamento de idéias de uma área para a outra permite um melhor entendimento do sistema e seu ambiente, e pode conduzir ao reconhecimento de riscos que poderiam ficar ocultos. A separação de propriedades facilita o reconhecimento de conflitos e compromissos.

O autor considera que a proposta feita por Eames e Moffett (1999) é válida, ou seja, uma integração parcial dos conceitos parece ser adequada, não reunindo os conceitos de Segurança Crítica e de Segurança de Informação em um único. Através dessa visão integrada, porém não unificada, torna-se possível continuar a se ter uma visão completa dos dois aspectos, sem a perda de detalhes importantes em cada uma das áreas abordadas. Esta opinião difere um pouco das opiniões emitidas pelo autor no item 4.1, mas atua como complemento às conclusões emitidas nesse item, quando da comparação dos principais conceitos sobre Sistemas Críticos e Sistemas de Informação**.**

Tribble (2002) não é partidário da junção dos dois conceitos de segurança. Para ele, a Segurança Crítica representa a ausência de condições que possam vir a causar acidentes. Esta é uma noção diferente da Segurança de Informação, que se constitui na habilidade de um sistema em resistir a riscos à sua operação, ou ainda, na habilidade de continuar a prover sua funcionalidade especificada, mesmo na presença de problemas.

Pode-se notar que Tribble é francamente contrário à idéia defendida pelos demais autores, cujas opiniões foram acima descritas, bem como à idéia central desta tese.

Segundo Winther (2001), muitos problemas relativos à Segurança de Informação também se configuram como sendo de Segurança Crítica, e só não são considerados

pela falta de metodologias para abranger problemas de Segurança de Informação no contexto de Segurança Crítica.

Este conceito vem de encontro à tese defendida neste trabalho de Livre Docência e acrescenta importância ao mesmo, ao levantar a questão da falta de metodologias para a consideração da Segurança de Informação em Sistemas Críticos.

Singh (1999) apresenta um contraste interessante entre Segurança Crítica e Segurança de Informação. A Segurança Crítica seria a prevenção de que a aplicação danifique o seu ambiente exterior em que estiver operando. A Segurança de Informação, por outro lado, representa a proteção do sistema contra danos causados a partir desse ambiente exterior. Desta forma, a Segurança Crítica representa a preocupação de não causar danos à vida, à propriedade e ao ambiente, enquanto que a Segurança de Informação representa a preocupação com a privacidade e correção dos dados.

Este conceito difere da tese defendida pelo autor, estabelecendo uma distinção marcante entre Segurança Crítica e Segurança de Informação.

Finalizando este item da integração dos conceitos, Ghosh (2002) aponta para os atentados terroristas de 11 de setembro de 2000 nos Estados Unidos, bem como outros ataques realizados a Sistemas de Informação, que acabaram por deixá-los fora de serviço. Segundo o autor, tais atentados devem servir como sinais de alerta urgentes para que a sociedade fique ciente do grau de vulnerabilidade a que a infraestrutura digital, vital a toda sociedade, está sujeita. Ghosh situa como Sistemas de Informação os sistemas de telecomunicações, transporte, energia, sistemas bancários e financeiros, sistemas governamentais e sistemas de emergência. Deixando fora do ar um ou vários desses sistemas, compromete-se em muito a economia e a segurança pública.

A posição de Ghosh vem de encontro à tese defendida pelo autor, situando diversos Sistemas de Informação como vitais à sociedade, podendo ser considerados, pelas conseqüências de suas falhas, como Sistemas Críticos.

4.2.2. Classificação dos Sistemas Críticos e Sistemas de Informação

Kotonya e Sommerville (1998) estabeleceram uma classificação dos Sistemas Críticos em três tipos principais: Sistemas Críticos de Negócios, Sistemas de Missão Crítica e Sistemas Críticos quanto à Segurança.

Sistemas Críticos de Negócios são aqueles nos quais uma falha pode causar prejuízos significativos aos negócios de uma organização. Um exemplo deste tipo de aplicação é o sistema de reserva de passagens de uma companhia aérea. Já uma falha nos chamados Sistemas de Missão Crítica pode comprometer o cumprimento de uma missão, como por exemplo, um problema no sistema de supervisão e controle de uma espaçonave. Finalmente, os Sistemas Críticos quanto à Segurança são aqueles nos quais falhas podem colocar em risco vidas humanas ou causar sérios danos ao ambiente. Como exemplo, pode-se citar um equipamento médico de tratamento por radiação.

Ainda segundo esses dois autores, seja qual for o tipo de sistema, a Segurança de Informação é um pré-requisito essencial para a Segurança Crítica. Não se pode estar confiante que uma aplicação respeita os requisitos de Segurança Crítica, se não se tiver também confiança de que seus dados não possam ser adulterados.

A classificação de Kotonya e Sommerville, que atribuem, aos Sistemas de Informação, a denominação de Sistemas Críticos de Negócios, vai na direção da fusão de conceitos, embora mantendo três categorias de Sistemas Críticos. Mais uma vez esta conceituação, aliada à afirmação de que a Segurança de Informação é um pré-requisito para a Segurança Crítica, vem de encontro à tese do autor, de reunir os conceitos de Sistemas Críticos e Sistemas de Informação nos chamados Sistemas Computacionais de Segurança.

Outra classificação é feita por Knight (2002), que questiona em seu artigo, o que são Sistemas Críticos. A preocupação, tanto intuitiva, quanto formal relaciona-se com as conseqüências das falhas. Se a falha de um sistema puder ocasionar conseqüências consideradas como inaceitáveis, então o sistema é classificado como sendo crítico quanto à segurança. As chamadas aplicações não tradicionais no que se refere à

Segurança Crítica, possuem potencial para ocasionar graves conseqüências, podendo também ser consideradas como Aplicações Críticas.

Por exemplo, a perda ou queda de um sistema de telefonia não tem maiores implicações de Segurança Crítica, a menos que se considere que também seja afetado o telefone de emergência da policia ou dos bombeiros, casos em que poderá haver ferimentos ou mortes em conseqüência dessa falha. Pode-se citar outros exemplos nas áreas de supervisão e controle de sistemas de transporte, sistemas financeiros e bancários, geração e distribuição de energia elétrica e gerenciamento dos sistemas de distribuição de água.

Dessa forma, segundo Knight (2002) torna-se prudente classificar os sistemas computacionais que controlam toda essa infraestrutura crítica como Críticos.

Verifica-se que há muitos sistemas utilizados para o projeto e manufatura de outros sistemas, nos quais as conseqüências de disfunções podem ser consideráveis. O software que fornece suporte ao desenvolvimento de outros programas, como, por exemplo, um compilador, é por si próprio crítico, se a aplicação a que ele irá servir também for crítica.

De acordo com Knight (2002), os Sistemas de Informação devem ser encarados dessa forma. Tomando como exemplo uma instituição financeira, a qual transfere valores localmente e ao redor do mundo, utilizando redes de comunicação privativas. Um ataque bem sucedido contra essas redes de comunicação pode permitir o furto, não apenas de fundos, mas também de informações como números de contas e de cartões de crédito, ou ainda interromper o fluxo de informações. Considerando-se que o potencial a perdas é muito grande, embora nenhum dano físico esteja diretamente envolvido, as conseqüências de falhas são tais que esses sistemas, cuja finalidade principal é transportar informações, podem ser considerados como críticos quanto à segurança, tendo em vista a importância de tais informações.

A opinião de Knight também vai na mesma linha de raciocínio do autor, estabelecendo a tendência de fusão das Aplicações Críticas e dos Sistemas de Informação, nas Aplicações Computacionais de Segurança.

Outra forma de classificação é proposta por Cullyer (1993), que destaca duas áreas de interesse. Uma primeira área é representada por sistemas bancários, de bolsas de valores e de mercadorias, bem como serviços financeiros. Em uma segunda área estão os sistemas embutidos, utilizados para controlar sistemas de transporte e grandes indústrias.

Se o mau funcionamento desses sistemas, seja de seu hardware, seja de seu software, puder provocar grandes perdas financeiras, colocar vidas do público em geral em risco, ou ameaçar com graves danos o ambiente, tais sistemas podem ser chamados de sistemas de alta integridade.

Segundo Cullyer (1993), esses sistemas de alta integridade devem possuir um Núcleo de Segurança de Informação representado por uma combinação de hardware e software, com a função de prevenir a obtenção ou mesmo a modificação não autorizada de dados, bem como prover suporte para a garantia de uma operação contínua, mesmo na presença de atos potencialmente maliciosos por parte de usuários.

Tais sistemas de alta integridade também devem contar com um Núcleo de Segurança Crítica, que representa uma combinação de hardware e software, cuja função é garantir e assegurar uma operação confiável e contínua. Assume-se que, nas Aplicações Críticas não haja ações maliciosas por parte de seus operadores e usuários e que as ameaças ao sistema são representadas por erros de projeto ou por operações acidentais.

Cullyer defende que ambos conceitos, da Segurança Crítica e Segurança de Informação, podem ser reunidos em um único chamado de integridade computacional.

O conceito de integridade computacional defendido por Cullyer tem o mesmo sentido da proposta de Sistemas Computacionais de Segurança e da Segurança Computacional, defendida pelo autor. Novamente, deve-se destacar, como no item anterior, que ações maliciosas podem ocorrer também em Sistemas Críticos.

4.2.3. Utilização de Computadores em Sistemas Críticos e em Sistemas de Informação

A utilização de computadores em Sistemas Críticos e em Sistemas de Informação apresentou um crescimento muito grande, a partir do momento em que suas vantagens econômicas e tecnológicas tornaram-se marcantes, vencendo o receio de seu emprego nessas áreas. O problema, a partir de então, consiste em mostrar que o emprego de computadores não vem sendo feito de forma precipitada e irresponsável, de maneira que não se exponham pessoas a riscos desnecessários (LEVESON, 1994)

Há a necessidade de haver uma certificação de Sistemas Críticos e Sistemas de Informação. Uma avaliação dos riscos é de fundamental importância para que se possa decidir sobre o uso ou não desse tipo de sistemas (DAPENA, 1999).

O autor concorda com o ponto de vista desses dois trabalhos, pois conforme já descrito nos capítulos 2 e 3, a utilização de sistemas de controle computadorizados já se constitui em prática comum, tanto em Sistemas de Informação, quanto em Sistemas Críticos, sendo que a realização de atividades de Análise de Segurança nesses sistemas sempre se faz necessária.

A preocupação com a segurança de sistemas computacionais, seja do ponto de vista da Segurança Crítica, seja do aspecto da Segurança de Informação, deve ser uma constante. Uma recomendação do governo americano especifica que conforme a economia e a sociedade vêm se tornando crescentemente dependentes da informatização, deve-se estar apto a projetar tais sistemas de forma mais segura e confiável (NATIONAL, 1999).

Esta preocupação do governo norte-americano vem de encontro à tese defendida pelo autor, colocando no mesmo nível de importância a Segurança Crítica e a Segurança de Informação.

Recomenda-se que o projeto de sistemas computacionais voltados a Sistemas Críticos seja feito considerando-se a existência de um núcleo pequeno e confiável que assegure a execução das funções consideradas mais críticas, mesmo no caso da ocorrência de falhas nos componentes externos a esse núcleo (SHA, 2001), (LI, 2001).

Esta é uma recomendação bastante útil, pois permite, se implementada, que maiores esforços de desenvolvimento sejam concentrados em módulos que realmente representem as funções críticas do sistema.

Com o aumento da complexidade de Sistemas Críticos e de Sistemas de Informação, o uso de controles automatizados também aumentou muito. Ao mesmo tempo, a função de operadores sofreu uma alteração, passando de responsáveis diretos pela operação completa dos sistemas para a supervisão ou monitoração dos mesmos. Dessa forma, reveste-se também de grande importância a preocupação da realização de projetos seguros no que se refere à interação homem-computador (BROWN, LEVESON, 1998).

Portanto, pode-se perceber que a utilização de sistemas computacionais em Sistemas Críticos e em Sistemas de Informação é uma tendência definitiva, sendo necessário que haja um projeto cuidadoso, a implementação seja feita de acordo com as normas vigentes e haja um processo de Análise de Segurança que considere não apenas o sistema, mas também o ambiente em que ele estiver inserido.

4.2.4. Análise de Requisitos em Sistemas Críticos e em Sistemas de Informação

Em um alto nível de abstração, o objetivo da Segurança Crítica e da Segurança de Informação é evitar e minimizar danos e perdas causados aos sistemas. Para contemplar esses objetivos, requisitos devem ser definidos na fase de análise de requisitos dos sistemas. Diferentes pontos de vista são usados para determinar cada domínio de requisitos (Segurança Crítica e Segurança de Informação).

Apesar desses domínios de exigência adotarem pontos de vista diferentes, o princípio básico dos conceitos de Segurança Crítica e Segurança da Informação é evitar que falhas possam explorar pontos fracos de um sistema, resultando em danos e perdas.

Um das contribuições mais importantes da Engenharia de Requisitos para a Segurança Crítica e a Segurança de Informação são os conceitos de requisitos primários e derivados (EAMES; MOFFETT, 1999). Em primeiro lugar deve-se considerar que equipes diferentes desenvolvem requisitos sobre Segurança Crítica e

sobre Segurança da Informação. Portanto, requisitos primários pertencem ao seu próprio domínio (por exemplo, requisitos de Segurança Crítica que afetam diretamente conceitos de Segurança Crítica, são definidos pela equipe de desenvolvimento dos aspectos de Segurança Crítica). Requisitos derivados pertencem ao outro domínio e são adotados para suportar os conceitos do primeiro domínio (por exemplo, requisitos de Segurança de Informação que afetam indiretamente conceitos de Segurança Crítica, tendo sido definidos pela equipe de desenvolvimento da Segurança de Informação).

Desta forma, este conceito de requisitos primários e requisitos derivados vai no sentido de se reunir os Sistemas Críticos e os Sistemas de Informação nos Sistemas Computacionais de Segurança.

4.2.5. O Aspecto Software em Sistemas Críticos e em Sistemas de Informação

O hardware de computador é projetado para ser de propósito geral, ou seja, necessita de um software associado para que possa realizar alguma função útil. O software carregado no computador é que determina a função que a máquina irá executar. A máquina torna-se de propósito específico durante o tempo de execução de um programa (SAFEWARE, 2002).

Pode-se dizer que o projeto de um software se constitui no projeto de uma máquina, considerando-se a abstração de sua realização física. A facilidade de se alterar um código de programa, e por conseqüência o propósito de um computador, constitui-se no grande benefício, e ao mesmo tempo na grande fonte de riscos do software. Alterando-se um código, altera-se também a função da máquina.

O software eliminou a maioria das restrições físicas existentes nos equipamentos anteriormente utilizados. Normalmente, quando se faz uma codificação, não há a preocupação, nem a correspondência direta, com a realização física de seus projetos, ou seja, quais são as correspondências efetivas entre o código implementado e a realidade física das aplicações.

Não há leis físicas que limitem, diretamente, a complexidade de um código de software, visto que o hardware ou a máquina de propósito geral praticamente não impõe restrições nesse sentido. Tais leis físicas, em projetos sem a utilização de computadores poderiam ser representadas por propriedades eletromagnéticas, forças estruturais, pontos de fusão, etc. Os fatores limitantes em um software são determinados pela criatividade de analistas e não por fatores físicos (SAFEWARE, 2002).

Um distúrbio em uma parte do sistema pode, potencialmente, afetar todas as demais partes do mesmo, em virtude da forma de supervisão e controle representada pelo software. O projetista perde a habilidade de antever possíveis conseqüências, em virtude da enorme complexidade atingida (LEVESON, 2000).

Outro problema que se coloca é que parte significativa dos novos projetos é representada pela realização de um programa. Desta forma, pode-se dizer que o projeto de novos equipamentos normalmente é feito por profissionais que não são especialistas nas áreas representadas pelos projetos, mas são especialistas em programação geral.

Pode haver uma falha inerente à programação. Há situações em que o software realiza exatamente o que estava especificado e mesmo assim não representa um programa seguro. Este fato normalmente ocorre porque não houve a previsão, na especificação do ambiente completo de execução ou operação (PIRIE, 1999).

Uma possível solução seria o uso de especificações formais e a prova dessas especificações por meio de lógica (GERHART, 1994). No entanto, há alguns problemas a serem considerados: a atividade de formalização teria o mesmo porte ou até seria maior do que a própria codificação, além de ser de construção mais difícil do que o código e de entendimento mais complexo.

Outro caminho seria encontrar meios de medir a qualidade de um software. Há diversos trabalhos nesse sentido, mas ainda não há consenso sobre quais características medir e se tais características teriam realmente impacto na segurança do software e do sistema associado.

Não há formas diretas de se medir o nível de confiabilidade ou mantenabilidade de um software. Uma alternativa para superar esta dificuldade é através da identificação de propriedades ou características internas mensuráveis que levem a esse objetivo maior, ou seja, a uma quantificação dessas qualidades externas (DROMEY, 1996).

Ainda outro caminho seria a realização de testes exaustivos nos programas, que se demonstra ser impraticável, tendo em vista o enorme número de casos de testes a serem realizados.

Por todos esses fatores apontados, pode-se dizer que o software representa ainda a maior fonte de dúvidas e problemas na implementação de Sistemas Críticos e de Sistemas de Informação.

4.3. Conclusões

Neste item destacam-se as principais conclusões que podem ser tiradas a respeito da aproximação dos conceitos mais relevantes sobre Sistemas Críticos e Sistemas de Informação, de forma a se poder considerar sua junção nos Sistemas Computacionais de Segurança. Da mesma forma, são analisados os aspectos da Segurança Crítica e da Segurança de Informação, também com o objetivo de verificar a possibilidade de fusão dos dois conceitos, resultando no conceito único de Segurança Computacional.

As considerações e conclusões apresentadas neste item vão no sentido de analisar a viabilidade de se considerar os Sistemas de Informação como possuindo, além de suas características peculiares, as características originárias de Sistemas Críticos. De forma similar, as considerações também vão no sentido de que os Sistemas Críticos venham a incorporar as características dos Sistemas de Informação, além de suas características próprias.

A base para a comparação feita neste item está em toda discussão feita no decorrer deste capítulo, comparando os diversos aspectos apresentados ao longo do texto para os dois tipos de sistemas.

Conforme toda a análise comparativa feita no decorrer deste capítulo, pode-se afirmar que há diversos aspectos que apontam para uma fusão, ainda que parcial e gradual, dos conceitos envolvidos em Sistemas Críticos e em Sistemas de Informação.

Esses aspectos comuns estão relacionados à forma de entendimento do próprio conceito de segurança, à aproximação que vem se observando na cultura de segurança, à forma de classificação dos sistemas e à grande importância que se atribui à obtenção de especificações corretas.

Há também aspectos que apontam para a direção inversa, ou seja, a de manutenção da separação dos conceitos. Os pontos que apresentam a maioria das divergências no que se refere a uma aproximação dos conceitos são a questão da implementação dos sistemas, as técnicas de análise de segurança, as normas atualmente existentes e as aplicações em si.

Pode-se dizer que o aspecto principal referente à comparação de Sistemas Críticos e Sistemas de Informação está na consideração de quão importante sejam as perdas decorrentes de falhas nesses sistemas. Torna-se cada vez mais aceito que perdas decorrentes em função de problemas que ocorram nos Sistemas de Informação tendem a causar graves conseqüências a seus usuários e à população de uma forma geral.

Portanto, a consideração da importância das perdas e a severidade das conseqüências de disfunções nos sistemas é que irão ditar o ritmo de adaptação dos Sistemas de Informação às características dos Sistemas Críticos.

Finalizando, por todos os conceitos, aplicações e exemplos descritos neste capítulo, pode-se dizer que já existe uma tendência de aproximação parcial, apontando para uma fusão gradual dos conceitos de Sistemas Críticos e Sistemas de Informação, gerando os Sistemas Computacionais de Segurança. O mesmo pode ser dito com relação à Segurança Crítica e à Segurança de Informação, criando o conceito de Segurança Computacional.

5. PESQUISAS REALIZADAS EM SISTEMAS CRÍTICOS E EM SISTEMAS DE INFORMAÇÃO

Neste capítulo são descritos os diversos trabalhos referentes às linhas de pesquisa relacionadas ao estudo de Sistemas Críticos e de Sistemas de Informação, dos quais o autor participou ou vem participando. Os resultados de cada um desses trabalhos de pesquisa se materializaram através da orientação e publicação de teses de doutorado, dissertações de mestrado, de artigos em periódicos e em congressos e projetos de pesquisa e extensão universitária.

Em cada uma das linhas de pesquisa apresentadas destaca-se a sua importância nos contextos da Segurança Crítica, Segurança de Informação, ou em ambas, além de serem descritos os principais aspectos relacionados a cada linha de pesquisa.

5.1. Orientações de Doutorado e Mestrado

Neste item são descritas as orientações a doutorandos e mestrandos, incluídas nos temas de Segurança Crítica e Segurança de Informação.

5.1.1. Identificação de Usuários através de Sistemas de Reconhecimento Biométrico

Esta linha de pesquisa seguida pelo orientado de mestrado do autor, Vilmar de Souza Machado, visa um aprofundamento no estudo da identificação de usuários através de sistemas de reconhecimento biométrico, assunto de fundamental importância no que se refere à identificação de usuários por parte de um sistema computacional.

Sistemas de reconhecimento biométrico são utilizados principalmente para a permitir ou não o acesso de usuários a um sistema ou a uma locação, quase sempre visando à garantia da Segurança Info-Crítica. Esta segurança pode ser simplesmente o controle de acesso físico a determinados locais, ou o controle lógico de acesso a um sistema computacional.

Desta forma, o tema desta dissertação de mestrado, na qual são descritos os principais aspectos referentes à proteção de sistemas através da utilização de

Sistemas de Reconhecimento Biométrico insere-se tanto na linha de pesquisa de Segurança Crítica, quanto na linha de Segurança de Informação do autor.

Nos itens a seguir são descritos os principais conceitos envolvidos, de maneira a possibilitar um entendimento mais amplo do assunto.

5.1.1.1. Reconhecimento Biométrico

Pode-se dizer que uma das habilidades humanas mais marcantes é o reconhecimento de seres humanos. O reconhecimento pode ser definido como um processo que envolve percepção e associação de informações com uma combinação de conteúdos armazenados na memória humana. A percepção visual captura informações de cenários específicos e essa percepção envolve alguns estágios do processamento da informação. A informação da imagem quando capturada pela retina é seguida por um processamento mental da imagem. A partir desse momento pode-se dizer que está ocorrendo o processo de identificação biométrica (CLARKE, 1994).

As duas principais fases do reconhecimento biométrico são a captura inicial da imagem para armazenamento em uma base de dados e a comparação com uma imagem posterior, quando algum usuário tentar acessar o sistema.

A primeira fase consiste no registro da informação biométrica no sistema, o que pode ocorrer através da captura da impressão digital, imagem da íris ou face, da captura da voz ou qualquer outra forma biométrica mensurável. O sistema não grava a foto do rosto ou a impressão digital. São coletados e armazenados apenas dados alfanuméricos criptografados.

A fase seguinte consiste na identificação do usuário. Uma característica biométrica deve ser decodificada e comparada ao padrão já armazenado no banco de dados. Raramente essa comparação indicará uma identidade total. Dessa forma, deve haver parâmetros que possibilitem a configuração do sistema, para que exista uma margem de tolerância que possa ser considerada aceitável, de acordo com cada tipo de aplicação.

Os sistemas biométricos utilizam alguma característica fisiológica ou alguma característica herdada pelos seres humanos. Para que o processo funcione é

necessário que a característica física a ser medida satisfaça aos seguintes requisitos (CLARKE, 1994):

- Universalidade: representa a necessidade de que praticamente todas as pessoas devam possuir a característica física a ser utilizada como medida;
- Singularidade: indica que a medida da característica física utilizada não deve ser igual em duas ou mais pessoas, ou no mínimo, que a probabilidade de haver duas pessoas com a mesma medida dessa característica seja muito pequena;
- Permanência: representa a propriedade de que a característica física selecionada não se modifique com o tempo;
- Mensurabilidade: consiste na possibilidade de se efetuar medidas quantitativas, tendo por base a característica física selecionada.

5.1.1.2. Formas de Reconhecimento Biométrico

As principais formas de reconhecimento biométrico atualmente utilizadas são a seguir descritas.

a) Reconhecimento da Voz

É a forma menos confiável, pois apresenta a maior probabilidade de erro, visto que um ruído no ambiente ou até mesmo uma rouquidão por parte do usuário já estariam prejudicando sua identificação.

Para capturar o som, o usuário pronuncia, preferencialmente, uma frase previamente selecionada. Esse processo é repetido diversas vezes até que se obtenha um modelo padrão. Deve-se levar em consideração, para que o reconhecimento seja possível, o usuário deve falar no tempo certo e de forma nítida.

b) Geometria Facial

Nesta técnica são delimitados vários pontos do rosto, identificando-se, por exemplo, a distância entre orelhas, olhos, maçãs do rosto, nariz e queixo. Mesmo com bigode, chapéu ou corte de cabelo diferentes, ainda é possível a identificação de um indivíduo.

A grande vantagem da utilização da técnica da geometria facial está na maneira como é capturada a imagem. A pessoa não precisa colocar o rosto em algum lugar exato e pré-determinado. Essa característica tem sido apresentada como um grande diferencial em relação a outras formas de reconhecimento biométrico, pois tem uma aceitação mais fácil por usuários que se utilizem dessa tecnologia.

c) Impressão Digital

É uma das formas de reconhecimento biométrico de menor custo, juntamente com o reconhecimento pela voz. Talvez seja por esse motivo que se constitui, atualmente, na técnica mais utilizada. Para o funcionamento desta forma de reconhecimento biométrico faz-se necessário um *scanner* de alta resolução, no qual a pessoa coloca o dedo para que seja feita a leitura dos traços e conseqüentemente a identificação.

Diversas empresas estão realizando grandes investimentos na evolução dessa tecnologia. Um dos empregos que já se nota é o acesso de usuários a sistemas operacionais, no lugar de se fornecer uma identificação e senha.

d) Assinatura

Nesta forma de reconhecimento biométrico o usuário deve repetir diversas vezes a sua assinatura para que o sistema possa obter um padrão médio, possibilitando o reconhecimento posterior. Este fato se constitui em um fator de inconveniência desta forma de reconhecimento biométrico.

Existe uma outra forma de reconhecimento através da assinatura que se constitui na dinâmica da assinatura. Nesse método o equipamento utilizado é a caneta óptica.

e) Retina

Pode-se dizer que é forma biométrica mais segura, ou seja, a que apresenta maiores dificuldades para o acesso de um usuário não autorizado. Mesmo que uma pessoa tenha doenças graves como glaucoma, ainda assim é possível sua correta identificação. Isso é possível porque o padrão de veias da retina é a característica com maior garantia de singularidade.

Este trabalho encontra-se em fase final de elaboração, tendo se aprofundado no estudo do reconhecimento biométrico pela impressão digital e pela geometria facial.

5.1.2. Arquitetura de Hardware Monoprocessado

A arquitetura de hardware utilizada em Sistemas Críticos se constitui em um importante fator de influência no que se refere à obtenção de níveis de segurança aceitáveis nesse tipo de aplicações. No capítulo 2 já foram descritos diversos tipos de arquiteturas utilizadas em Aplicações Críticas. Neste item é descrita uma nova proposta de implementação, feita pelo orientado do autor, José Antonio Fonseca, em sua dissertação de mestrado (FONSECA, 2001).

Portanto, o tema dessa dissertação de mestrado insere-se na linha de pesquisa da Segurança Crítica, seguida pelo autor. Nessa dissertação, já concluída, são descritos os principais aspectos referentes a uma proposta de implementação de um Sistema Crítico, utilizando apenas um processador em sua arquitetura.

Este mesmo orientado, José Antonio Fonseca, vem realizando o doutorado, também na linha de pesquisa de Segurança Crítica, sendo que detalhes desta nova pesquisa são apresentados no item 5.1.7.

Nos próximos itens são descritos os principais conceitos envolvidos, de maneira a possibilitar um entendimento mais amplo do assunto.

5.1.2.1. Proposta de um Sistema Monoprocessado

No projeto de um Sistema Crítico, há precauções adicionais a serem seguidas se for utilizada apenas uma unidade processadora. Neste caso, é de vital importância a existência de diagnósticos no sistema, de tal forma que seja possível a detecção, senão de todas, pelo menos de parcela significativa das falhas que possam ocorrer no sistema. Essa capacidade de detectar falhas recebe o nome de Fator de Cobertura de Falhas.

O Fator de Cobertura é determinado por testes existentes no software e no hardware do Sistema Crítico. Nas arquiteturas com redundância de unidades processadoras, o Fator de Cobertura de Falhas é aumentado pela comparação dos resultados entre as

unidades replicadas, o que não é possível no caso de haver apenas uma unidade processadora.

A forma de implementação proposta sugere a utilização de um único processador que tem a função de executar duas versões de software, cuja funcionalidade deve ser a mesma. As versões do software podem, em princípio, serem réplicas de um mesmo programa. No entanto, o ideal é que sejam implementações distintas originadas a partir de uma mesma especificação.

A arquitetura proposta sugere a adição de um segundo processador, muito mais simples do que o processador principal, tendo assim a propriedade de aumentar o Fator de Cobertura de Falhas. Esse segundo processador pode ficar observando o comportamento do processador principal, bem como o processador principal pode também supervisionar o funcionamento desse processador auxiliar. Em caso de qualquer problema, deve haver a respectiva sinalização pelo processador que detectou a situação. O processador auxiliar recebe a denominação de Processador *Watchdog*, e a arquitetura do sistema é apresentada na figura 5.1.

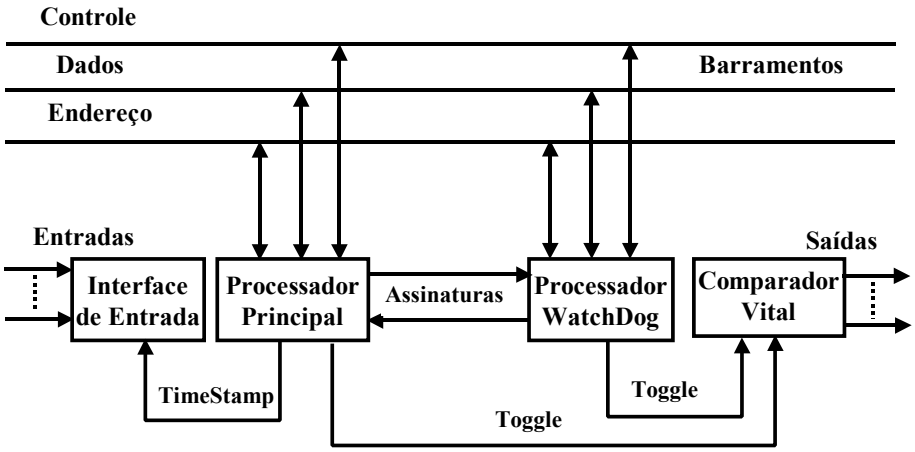

Figura 5.1 - Arquitetura Monoprocessada

O processador principal é responsável pela realização das funções críticas da aplicação em questão. Sua arquitetura pode ser do tipo RISC, com *pipeline* e *cache* interno, de forma a melhorar o desempenho. Isto se faz necessário, tendo em vista que o processador principal deve executar duas réplicas do software e ainda atender aos requisitos de tempo da aplicação.

O grau de complexidade do processador principal não afeta significativamente a Segurança Crítica. A norma MIL-HDBK-217F (MILITARY, 1990) não considera que um aumento no número de unidades funcionais do processador aumente sua taxa de falhas. Essa norma considera como fator relevante o número de bits no barramento de dados.

O processador principal tem uma saída chamada de *TimeStamp*, utilizada pelos dispositivos de entrada, atribuindo às entradas uma marca de tempo, imprimindo uma característica dinâmica aos valores das entradas. O Processador Principal verifica se o Processador *WatchDog* está realizando seu processamento de forma correta, utilizando como diagnóstico um conjunto de assinaturas geradas pelo Processador *WatchDog*. O mesmo é feito pelo Processador *WatchDog* em relação ao Processador Principal. Se for detectado qualquer tipo de falha por qualquer um dos dois processadores, as saídas do bloco Comparador Vital são desabilitadas pelos sinais de *Toggle*.

As Interfaces de Entrada recebem dados do campo, realizando seu processamento de forma duplicada, por circuitos independentes.

A função básica do Processador *WatchDog* é supervisionar o funcionamento do Processador Principal e inibir a geração de saídas pelos Comparadores Vitais, se alguma falha for detectada. A técnica de utilização de um Processador *WatchDog* é baseada em uma técnica mais geral chamada de *safety bag* (IEC, 1997).

O Processador *WatchDog* tem um número de modos de falha muito menor do que o Processador Principal. Também pode ser usado para detectar erros causados pelo software do Processador Principal, através de verificações sobre a consistência dos resultados gerados. O emprego do Processador *WatchDog* fornece diversidade ao hardware, proporcionando proteção contra erros de modo comum e independência na verificação do Processador Principal (MAHMOOD; McCLUSKEY, 1988).

5.1.2.2. Comparação entre as Arquiteturas

O custo de implementação de uma arquitetura duplicada é basicamente o dobro de uma arquitetura que utilize apenas uma unidade de processamento, sem se considerar o custo adicional de estruturas mecânicas para acomodar a configuração duplicada. Outro fator a ser considerado é que a taxa de falhas da arquitetura duplicada é o dobro da taxa de falhas de uma arquitetura monoprocessada (SIEWIOREK; SWARZ, 1992).

A arquitetura com apenas uma unidade de processamento tem um custo menor e uma confiabilidade mais alta, quando comparada com a arquitetura duplicada. No entanto, para Aplicações Críticas, a arquitetura monoprocessada tem um tempo médio entre falhas inseguras muito menor, quando comparada com a arquitetura duplicada.

A forma de solucionar tal problema é reduzir a taxa de falhas inseguras da unidade monoprocessada, tornado-a equivalente à da arquitetura duplicada. Na arquitetura proposta, isto é obtido através de um aumento no fator de cobertura do software.

5.1.3. Bases de Dados Distribuídas

A utilização de bases de dados distribuídas é cada vez mais uma necessidade, tendo em vista que os empreendimentos vêm demonstrando tal vocação, ou seja, de se distribuírem conforme as diversas áreas dentro de uma organização. A distribuição dos dados não pode ser feita sem um estudo prévio detalhado, sob o risco de se passar a ter bases de dados de acesso ineficiente, bem como diversos problemas de replicações desnecessárias ou ainda falta de replicações. Desta forma, este trabalho de tese de doutorado, já encerrado, do orientado do autor, Pedro Luiz Pizzigati Correa descreve uma pesquisa na qual são propostas diretrizes e procedimentos para que o projeto de distribuição dos dados possa ser feito da maneira mais eficiente possível, inserindo-se na linha de pesquisa de Sistemas de Informação (CORREA, 2002).

Neste item são descritos os principais conceitos envolvidos, de maneira a possibilitar um entendimento mais amplo do assunto.

O projeto de uma Base de Dados Distribuída envolve vários processos, desde a concepção do projeto inicial de distribuição, o monitoramento do projeto durante sua operação, avaliação de possíveis alterações, e até se necessário, a redefinição do projeto de distribuição.

Deve-se ressaltar a importância do processo de coleta de parâmetros, uma vez que a qualidade do projeto de distribuição está diretamente relacionada com a precisão dos parâmetros obtidos pelo projetista.

Os parâmetros usados no projeto de distribuição podem ser estimados pelo projetista ou obtidos através de um processo de monitoramento. O projetista pode estimar parâmetros lógicos ou físicos com o objetivo de gerar um projeto inicial ou mesmo para permitir avaliar soluções alternativas, de acordo com variações aplicadas nos parâmetros do projeto. Já o processo de monitoramento deve ser considerado para verificar o desempenho da implementação, tendo em vista possíveis revisões de projeto.

As Diretrizes e Procedimentos definidas nesse trabalho são válidas para aplicações do tipo OLTP (*On-Line Transaction Processing*), para Bases de Dados que utilizam o Modelo Relacional, em um ambiente de distribuição em que não existam grandes disparidades de capacidade de processamento nem de velocidade de comunicação de dados entre os nós, distribuídos.

As estratégias e os procedimentos apresentados podem ser aplicados tanto para definir o projeto inicial, a partir de parâmetros estimados pelo projetista, como para um re-projeto da base de dados, a partir de parâmetros obtidos de monitoramento.

O projeto de distribuição é aplicado nas relações globais relevantes, ou seja, aquelas com maior utilização. O projeto de distribuição das demais relações é definido em função das relações globais relevantes, considerando os relacionamentos existentes entre elas.

Nem sempre será necessário fragmentar todas as relações globais relevantes. Por exemplo: relações que têm um volume de dados pequeno, ou só são acessadas por transações localizas em um mesmo nó, não devem ser fragmentadas. Outras situações relacionadas com a segurança dos dados ou mesmo com a facilidade de

administração, identificadas pelo projetista, devem ser consideradas durante a análise. Dessa forma, foi acrescentada uma fase de análise inicial, que tem por objetivo identificar a necessidade da fragmentação de uma relação, antes de aplicar os métodos de fragmentação (horizontal e vertical).

A forma de alocação de fragmentos adotada neste trabalho tem por objetivo geral encontrar uma solução que minimize o tempo de resposta das aplicações e os custos de execução da aplicação.

As diretrizes e procedimentos propostos neste trabalho foram aplicados a uma base de dados centralizada da Secretaria da Fazenda do Estado de São Paulo. A implementação propriamente dita não foi realizada, embora os resultados teóricos tenham indicado uma grande melhoria de desempenho em relação à base de dados centralizada existente.

5.1.4. Modelagem Multidimensional de Dados

A modelagem de dados constitui-se em uma das principais ferramentas no desenvolvimento de Sistemas de Informação e, por conseqüência, na Segurança dos Dados integrantes desses sistemas, bem como na melhoria de seu desempenho. A modelagem de um Data Warehouse também se insere nesse contexto, visto que quanto mais um modelo representar os requisitos exigidos pelos usuários, maior a satisfação com o sistema. No capítulo 3 foram descritas as principais características que compõem um Data Warehouse.

Desta forma, o trabalho do orientado de mestrado do autor, Pedro Willemsens, já concluído, descreve uma proposta de uma nova forma de modelagem multidimensional para Data Warehouses, a partir do modelo relacional utilizado para Bases de Dados transacionais (WILLENSENS, 2002). Portanto, o tema dessa dissertação de mestrado insere-se na linha de pesquisa de Sistemas de Informação.

A proposta desse novo modelo multidimensional é feita através de conjuntos, relações e sentenças lógicas de primeira ordem, bem como há uma forma gráfica de se representar o modelo, através de diagramas.

Em bancos de dados relacionais, as formas normais desempenham um papel importante de avaliação e aprimoramento dos modelos de dados. Estas definem propriedades que, se atendidas, garantem à base de dados um bom funcionamento. Uma base modelada fora das características definidas pelas formas normais, provavelmente terá problemas de redundância (resultando no uso de um espaço de armazenamento desnecessário), atualizações inconsistentes, anomalias de inclusão e de supressão de elementos. Assim, as formas normais definem boas modelagens, evitando os problemas citados.

De certa forma, a própria existência de formas normais revela certa fraqueza do tipo de modelo de dados que se está utilizando. Estas são uma prova de que o modelo dá mais liberdade de modelagem do que seria interessante, permitindo que se faça modelos ruins. O que a definição do tipo de modelo de dados (no caso o relacional) não consegue garantir estruturalmente, é preciso que seja recomendado ao projetista usuário do modelo como uma boa prática de modelagem.

Para o modelo multidimensional proposto também acontece algo semelhante ao que gerou a necessidade de definição de formas normais para o modelo relacional. Desta forma, no trabalho, também é feita uma proposta para a normalização do modelo proposto.

Descreve-se também, na dissertação, um algoritmo que permite a obtenção do modelo multidimensional proposto, a partir de uma base de dados relacional.

5.1.5. Arquitetura de Hardware para Sistemas Computacionais de Segurança

A arquitetura de hardware utilizada em Sistemas Críticos e em Sistemas de Informação necessita de um alto nível de redundância, de forma que se possa assegurar os níveis de segurança, confiabilidade e disponibilidade exigidos para tais aplicações. A redundância no armazenamento de dados é um fator que exerce forte impacto tanto em Aplicações Críticas, quanto em Sistemas de Informação, pois ambos tipos de aplicações necessitam contar com disponibilidade praticamente total, bem como a confiabilidade das informações armazenadas deve ser a maior possível.

Dentro desse contexto é que se enquadram os Sistemas de Armazenamento do tipo RAID – *Redundant Array of Inexpensive Disks*, que se constituem na principal forma de armazenamento redundante de dados utilizada em sistemas de grande responsabilidade. Este estudo foi desenvolvido pelo orientado do autor, Enderson Ferreira, em sua dissertação de mestrado.

Portanto, o tema dessa dissertação de mestrado insere-se tanto na linha da Segurança Crítica, quanto na linha de Segurança de Informação.

Os dispositivos de armazenamento de dados utilizados em aplicações que necessitem de grandes taxas de segurança, confiabilidade e disponibilidade, devem possuir mecanismos adicionais que suportem a tolerância a falhas dos meios de armazenamento e de seus dispositivos de controle. O principal mecanismo empregado é o da Replicação de Dados, que consiste no armazenamento dos dados em mais de uma locação de memória ou de disco. A replicação pode ocorrer simplesmente através de uma cópia dos dados ou ainda através de alguma operação lógica que se faça necessária sobre os dados originais.

Uma das técnicas mais comumente utilizadas para a implementação da redundância de dados ocorre através da utilização das arquiteturas RAID - *Redundant Array of Inexpensive Disks*.

Pode-se afirmar que o conceito de implementação de sistemas computadorizados não tem mais o seu foco central voltado para as unidades de processamento, mas sim para os sistemas de armazenamento secundário (COURTRIGHT, 1997).

Uma matriz de discos redundantes consiste em um conjunto de discos magnéticos (discos rígidos) acoplados entre si, formando uma única unidade lógica do ponto de vista do sistema computacional (PATTERSON; HENNESSY, 1990).

As arquiteturas RAID utilizadas alocam uma porção de sua capacidade para armazenamento de códigos redundantes, que permitem a recuperação dos dados originais, no caso de falha de algum disco da arquitetura, a partir dos dados presentes nos demais discos (SCHULZE et al., 1988).

Embora a redundância presente em uma arquitetura RAID possa servir também para um aumento do desempenho de um sistema, seu principal atrativo está na melhoria da segurança, confiabilidade e disponibilidade dos dados armazenados.

A partir da identificação da ocorrência de falha em um disco da arquitetura RAID, faz-se necessário executar o processo de reparo do sistema. Esse processo de reparo de um disco falho envolve dois componentes de tempo: o tempo gasto para substituição do dispositivo e o tempo para remontagem dos dados a partir dos dados contidos nos demais discos da arquitetura.

Discos reservas *online* ou a substituição de discos sem a necessidade de desligamento da máquina são técnicas utilizadas para minimizar esse tempo e tornar sistemas de informação mais confiáveis e disponíveis.

As arquiteturas RAID podem ser classificadas em sete níveis (PATTERSON; HENNESSY, 1990):

- RAID 0: não contém nenhum tipo de redundância ou de paridade dos dados, ocorrendo apenas o entrelaçamento ou distribuição dos dados em diversos discos;
- RAID 1: nesta classe de redundância de discos, é feito o espelhamento dos dados em um ou mais discos distintos;
- RAID 2: consiste na implementação do armazenamento dos dados através de Códigos de Hamming, que possibilitam a correção de erros, de acordo com o nível de redundância utilizado;
- RAID 3: nesta classe de redundância, há um disco exclusivamente dedicado ao armazenamento da paridade dos dados, calculada em todos os demais discos da matriz redundante;
- RAID 4: realiza-se o armazenamento de blocos de dados de forma entrelaçada entre os diversos discos da arquitetura, sendo que um dos discos continua reservado ao armazenamento do bit de paridade;
- RAID 5: nesta classe também se realiza o armazenamento de blocos de dados de forma entrelaçada entre os diversos discos da arquitetura, bem como o armazenamento da paridade também é distribuído entre os diversos discos; e

- RAID 6: tem as mesmas características do RAID nível 5, além de apresentar também redundância de dados.

Neste trabalho, cada uma das arquiteturas RAID é modelada por intermédio das técnicas Redes de Petri ou por Modelos de Markov, obtendo-se as expressões para a confiabilidade de cada tipo de implementação, permitindo-se a seleção da arquitetura mais conveniente a ser utilizada.

5.1.6. Bases de Dados Aplicadas à Segurança Crítica

Um ponto importante a ser considerado são as relações entre os pontos de vista da Segurança Crítica e da Segurança de Informação na área de bases de dados, sendo que muitos conceitos de análise de segurança mesclam essas duas linhas, porém não há uma formalização ou estudos que deixem claras as limitações de cada uma. Desta forma, esta linha de pesquisa seguida pelo orientado de mestrado do autor, Ricardo Alexandre Veiga Gimenez irá abordar este importante aspecto.

O processo de segurança deve começar com uma compreensão clara de qual informação necessita ser protegida, de forma a possibilitar um projeto seguro para uma base de dados.

Para fornecer confiabilidade a uma base de dados, uma análise de segurança deve ir além de proteger a informação. Um aspecto importante a ser pesquisado é que os fornecedores de ferramentas de gerenciamento de bases de dados costumam confundir os conceitos de confiabilidade e disponibilidade. Assim, quando um fornecedor divulga um determinado valor para a confiabilidade de seu gerenciador, na realidade está fazendo referência à sua disponibilidade.

Existem muitas aplicações que se preocupam com a Segurança de Informação em bases de dados. Este fenômeno ocorre principalmente pelo fato de que os principais usuários de grandes Sistemas de Informação são instituições bancárias. Do ponto de vista de tais instituições, a disponibilidade é um fator essencial, porém um erro em um dado não implica em risco de vida como em uma Aplicação Crítica. Por outro lado, em sistemas do tipo aeronáutico, que também utilizam grandes quantidades de

dados, qualquer falha pode levar a situações de perigo, com possibilidades de ocasionar vítimas fatais.

O objetivo deste trabalho será o de procurar mostrar possíveis caminhos para que se possa garantir que um Sistema de Informação baseado em uma grande base de dados possa ser confiável, seguro e ao mesmo tempo disponível.

Para que seja possível desenvolver um estudo completo sobre esse tema, é necessário investigar o caminho completo seguido pelos dados em um sistema. Na entrada de dados é feita sua padronização. A utilização de normas para a codificação e acesso aos dados é essencial. A saída de informação pode requerer o cruzamento de dados, que, se mal planejados, podem fornecer falsas afirmações.

Algumas linhas de pesquisa a serem seguidas são:

- Desenvolvimento de Sistemas Robustos através da utilização de ferramentas comerciais de prateleira, através do desenvolvimento de interfaces mais robustas, tendo em vista tais ferramentas não permitem adaptações internas.
- Análise de Desempenho: definição de critérios e avaliações de desempenho, procurando um balanceamento entre confiabilidade e disponibilidade.
- Avaliação de Sistemas Transacionais: definição das fronteiras de atuação.

5.1.7. Modelo de Desenvolvimento para Aplicações Críticas quanto à Segurança

O software de Sistemas Críticos é o componente que mais tem atraído a preocupação, pois o histórico de falhas em sistemas desse tipo indica que o software tem grande parcela de responsabilidade nas mesmas.

Nos últimos anos muitas técnicas foram desenvolvidas para o projeto e avaliação quantitativa dos níveis de segurança do hardware de sistemas, mas, até o presente momento, nenhuma técnica de avaliação quantitativa satisfatória foi desenvolvida para a análise de segurança de software.

O fato de não existirem técnicas apropriadas para avaliação quantitativa da confiabilidade e segurança de software levou à criação de técnicas qualitativas de

avaliação e de metodologias de desenvolvimento de software onde a segurança e a confiabilidade são garantidas através do emprego da engenharia de software e de conceitos de qualidade de software.

Hoje é consenso entre os especialistas que a aplicação de processos disciplinados no desenvolvimento de software contribui para o aumento da qualidade do produto (KRISHNAN; KELLNER, 1999).

Ao longo do tempo, especialistas elaboraram uma lista de boas práticas de construção de software e criaram programas com o intuito de auxiliar as empresas a avaliarem seus processos e a promoverem melhorias dos mesmos.

O SPI (*Software Process Improvement*), é um movimento neste sentido com o objetivo promover a melhoria através do rompimento de valores tradicionais enraizados no modo de construir software, ajudando as empresas a localizarem os problemas de seus métodos, incentivando a criação de conhecimento, encorajando a participação de seus desenvolvedores no processo, integrando lideranças em torno da causa e criando a cultura de planejamento de melhoria contínua.

Existem vários programas de SPI (MATHIASSEN, 2001) como o SPICE (S*oftware Process Improvement and Capability dEtermination*), SPIRE (*Software Process Improvement in Regions of Europe*), SEI – CMM (*Capability Maturity Model*) e *Bootstrap*.

Dentre estes, o CMM alcançou notoriedade e tem sido implementado em várias organizações. O CMM é uma estrutura que descreve quais etapas são necessárias para que uma organização de software produza, consistente e previsivelmente, produtos de qualidade assegurada. Devido a essa busca por qualidade, e que tem seu enfoque voltado para a medição da maturidade de capacitação, que consiste em analisar o quanto o processo é capaz de assegurar a qualidade dos produtos gerados, obter a confiabilidade na gerência do projeto, incrementar o grau da capacidade de adaptação às características da empresa e dos projetos, bem como estar apto a constantes mudanças.

Desta forma, o objetivo desta tese de doutorado do orientado do autor, José Antonio Fonseca é o de propor um modelo de maturidade voltado principalmente para o

aspecto da Segurança Crítica. Será uma espécie de CMM destinado a Sistemas Críticos.

5.2. Demais Linhas de Pesquisa

Neste item são descritas as demais linhas de pesquisa seguidas pelo autor, ligadas à Segurança Crítica e à Segurança de Informação.

5.2.1. Programação Defensiva

Esta atividade de pesquisa visa mostrar a grande importância que existe em se estudar a utilização dos conceitos de Programação Defensiva, principalmente no que diz respeito à Segurança Crítica (ALMEIDA et al., 2002b).

No contexto de Sistemas Críticos, a programação defensiva é uma técnica que pode ser usada para a prevenção de falhas de software, de hardware e a ocorrência de entradas inválidas, levando o sistema a um estado seguro, quando for verificada uma dessas condições.

Eventos tais como entrada de dados errônea pelo usuário (por exemplo, entrar um dado no formato incorreto), problemas de entrada e saída de arquivos (por exemplo, fim de arquivo ou disco sem espaço), problemas de operações aritméticas (por exemplo *overflow*), interrupções de hardware e de software (por exemplo, pressionar a tecla *break*) podem ser previstos no projeto do software, constituindo a chamada programação defensiva.

O método de utilização de técnicas de programação defensiva consiste na adição de asserções, verificações, etc., no código, de forma a detectar erros, saindo da execução normal do programa ou tomando alguma ação corretiva, dependendo da severidade da falha.

Técnicas de programação defensiva baseiam-se na suposição de que o hardware e o software do sistema não são totalmente confiáveis e, portanto, podem vir a apresentar comportamento não esperado (CHENG et al., 1990).

Contudo, tais regras não são suficientes para que se obtenha um código com a qualidade suficiente. Técnicas adicionais devem ser consideradas na atividade de codificação. Tais atividades são conhecidas como técnicas de programação defensiva e devem estar presentes em Sistemas Críticos, incrementando suas características de robustez.

Algumas das principais técnicas utilizadas na programação defensiva são (ALMEIDA et al., 2002b):

Teste de Valores Válidos: é conveniente testar todos valores utilizados no código de forma a verificar se estão dentro das faixas de valores consideradas como válidas.

Teste de Sincronismo: eventualmente, a execução de algumas rotinas deve obedecer a um sincronismo com outras rotinas, assegurando uma correta seqüência de eventos.

Teste de Tempos de Execução: em alguns casos não é suficiente verificar se os resultados estão corretos, mas também deve-se verificar se os tempos de geração dos mesmos estão dentro de padrões pré-especificados.

Verificação da Capacidade: o hardware dos computadores tem limitações estabelecidas por fatores físicos dos circuitos, tais como dispositivos de entrada/saída. Dessa forma, a capacidade máxima de todos os dispositivos físico do computador não deve ser excedida.

Teste de *Time-outs*: Se o tempo de geração de algum sinal de saída for excedido, alguma ação preventiva deve ser tomada para regularizar o fluxo de processamento.

Teste de Áreas de Memória: um dos principais problemas a ser evitado é a utilização de áreas restritas de memória. Assim sendo, o uso da memória deve ser precedido por testes de endereçamento, assegurando acesso correto a dados ou ao código.

Tratamento de Exceções: exceções consistem em condições de erro não esperadas que ocorrem durante o tempo de execução dos programas, tais como divisão por zero, *overflow*, etc. Tais condições são detectadas automaticamente pelos mecanismos de detecção, sinalizadas e tratadas pelos mecanismos de tratamento. Tais mecanismos podem ser estabelecidos pelos próprios programas dos usuários, sendo disparados quando uma condição de exceção for sinalizada.

Verificação de Argumentos de Funções: este tipo de técnica verifica se os argumentos de uma função estão dentro de limites pré-determinados. A verificação de argumentos é uma técnica que consome um tempo razoável de processamento, especialmente se determinada função é acionada com grande freqüência.

Códigos de Retorno de Erros: funções podem retornar códigos de erro quando da detecção de condições de erro no processamento. A geração desses códigos pode alertar a equipe de manutenção a tomar as ações necessárias. Portanto, é importante especificar e implementar corretamente as condições a serem analisadas, bem como os códigos de erros gerados.

Retorno de Subrotinas: quando uma rotina é chamada, deve ter o código necessário para que se assegure que após o retorno à rotina acionadora, o processamento prossiga sem perdas, assegurando a correta continuidade. Se houver rotina com procedimentos incorretos de retorno, outras rotinas do software poderão ter seu processamento afetado, executando ações de forma incorreta.

Controle de Laços: a terminação de laços deve ser corretamente implementada de forma a evitar a execução de forma infinita de um trecho de código. A não terminação de laços pode ocasionar a não ativação de funções de segurança crítica, quando necessário, podendo levar o sistema a situações perigosas. Também é importante assegurar a correção das condições de controle do laço, evitando que algum trecho de código não seja executado, quando isto seja necessário.

Testes de Entrada/Saída: as seções iniciais e finais das rotinas devem incluir testes que garantam a correta entrada e saída de cada rotina. Esta providência faz-se útil para evitar a reentrância causada por desvios impróprios que possam antes do final de rotinas ou diretamente para o meio de rotinas.

5.2.2. Lista de Inspeção

Um aspecto de extrema importância em sistemas computadorizados é que, mesmo que o software faça exatamente o que foi especificado, pode ainda assim não ter a propriedade da Segurança Crítica, se o ambiente de funcionamento não for conhecido ou previamente avaliado (PIRIE, 1999).

Uma das atividades da verificação da Segurança Crítica se constitui no processo de inspeção do código fonte utilizado em Aplicações Críticas. A inspeção do código é uma das tarefas realizadas no processo mais geral que é a Análise de Segurança da Aplicação, e se constitui em outra atividade de pesquisa desenvolvida pelo autor, ligada a Sistemas Críticos.

Inspeções formais de software podem detectar e eliminar erros produzidos ao longo do ciclo de desenvolvimento do software. O uso de listas de inspeção é uma técnica para identificar falhas (GILB; GRAHAM, 1994). A lista representa uma relação das classes de falhas mais gerais que devem ser verificadas. Através da inspeção, falhas podem ser detectadas e eliminadas por meio de correções no código. Uma lista de inspeção deve contemplar todos tipos ou sintomas de falhas, assistindo a equipe de desenvolvimento em sua atividade (BIFFL;HALLING, 2000), (WALKER, 1997).

É importante destacar que a lista de inspeção pode ser útil a outras questões também bastante significativas, como por exemplo, a tolerância a falhas. Se todos itens da lista forem respeitados, também se estará aumentando a propriedade da tolerância a falhas do sistema.

Outro aspecto é a Segurança de Informação, que conforme apontado guarda estreita relação com a Segurança Crítica. Certamente os itens presentes na Lista de Inspeção cobrem também aspectos relativos à Segurança de Informação.

Se a técnica de listas de inspeção for empregada de forma sistemática, diminui-se a probabilidade de intersecção entre as falhas detectadas, aumentando a efetividade da inspeção (PORTER; VOTTA, 1998). A Lista de Inspeção é um conjunto de questões que dirige o processo de Análise de Segurança.

Os principais tópicos constantes de uma Lista de Inspeção são muito semelhantes àqueles já descritos para a linha de Programação Defensiva, no item anterior, não sendo, portanto aqui reproduzidos (ALMEIDA et al., 1999), (ALMEIDA et al., 2000).

5.3. Aplicações e Projetos de Pesquisa e de Extensão

Neste item são descritos os projetos de pesquisa e de extensão universitária dos quais o autor vem tendo participação, ambos relacionados às linhas de pesquisa de Sistemas Críticos e Sistemas de Informação.

5.3.1. Cia do Metropolitano de São Paulo

A Cia do Metropolitano de São Paulo vem demonstrando, praticamente desde a sua implantação, uma preocupação constante no que se refere à segurança na operação de suas linhas. As linhas do Metrô de São Paulo são controladas por equipamentos especialmente desenvolvidos que contêm processadores em seus circuitos, tanto no que se refere a equipamentos embarcados nos trens, quanto a equipamentos distribuídos ao longo da via.

Dessa forma, ocorre que a cada novo Sistema de Supervisão e Controle para a movimentação dos trens em suas linhas, ou mesmo a cada modificação efetuada nesses sistemas, a Cia do Metropolitano de São Paulo vem recorrendo ao Grupo de Análise de Segurança – GAS, Laboratório de Pesquisa pertencente ao Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da USP, do qual o autor faz parte ativa, sendo um de seus coordenadores. O GAS efetua então a análise de segurança dos equipamentos e sistemas novos ou modificados, indicando eventuais condições perigosas que sejam detectadas no hardware e software analisados.

Por exemplo, pode-se citar que um dos primeiros Sistemas de Supervisão e Controle de Movimentação de Trens totalmente computadorizado, a nível mundial, foi instalado no Metrô de São Paulo. A análise de segurança desse sistema foi feita pelos pesquisadores do Grupo de Análise de Segurança. Inicialmente esse sistema de

controle e movimentação de trens foi instalado no Pátio de Manobras de Itaquera. Comprovada a sua eficácia, tanto através de sua operação, quanto da análise de segurança, a utilização de tal tecnologia vem sendo constantemente expandida a linhas comerciais, como a Linha 2 – Verde (Ramal Paulista) e a nova Linha 5 – Lilás (Largo Treze) (Cia do METROPOLITANO, 2003)

Dessa forma, todo o estudo efetuado pelo autor na linha de Sistemas Críticos e de Sistemas de Informação encontra uma aplicação moldada na medida exata para que se possam empregar todos os conceitos pesquisados.

Pode-se dizer que o estudo e análise de segurança, tanto dos equipamentos embarcados nos trens, quanto dos equipamentos distribuídos ao longo da via possibilitou, por um lado a aplicação dos conceitos estudados, e por outro lado, incentivou a realização de novas pesquisas, tendo em vista novas necessidades identificadas em uma aplicação prática.

A operação de uma linha do Metrô apresenta todas as características de uma Aplicação Crítica, pois falhas em seu Sistema de Supervisão e Controle podem provocar perdas materiais de vulto, em caso de colisão ou descarrilamento de trens, e evidentemente causar ferimentos ou perdas fatais entre seus usuários e operadores.

Como complemento, vale a pena destacar algumas características da malha metroviária controlada pela Companhia do Metropolitano de São Paulo. Atualmente, o Metro de São Paulo tem 4 linhas, totalizando 57,6 km de extensão, com um total de 21 estações. Possui 702 carros em sua na frota, sendo 618 utilizados nos horários de pico. O intervalo mínimo entre trens é de 101 segundos na Linha 3 – Vermelha (Leste-Oeste). Em 2001 houve um total de 503 milhões de passageiros em todas as linhas, resultando em uma média de 1,378 milhões de pessoas/dia. Considerando-se apenas os dias úteis, este número sobe para 1,7 milhões de pessoas/dia (Cia do METROPOLITANO, 2003).

5.3.2. CNS/ATM - *Communication, Navigation and Surveillance/Air Traffic Management*

O gerenciamento de tráfego aéreo denominado ATM (*Air Traffic Management*) é responsável pelo controle de aeronaves em um determinado espaço aéreo, que é subdividido em setores controlados por Centros de Controle de Tráfego Aéreo, denominados ATC (*Air Traffic Control*), responsáveis pela coordenação e resolução de conflitos no espaço aéreo sob sua responsabilidade. O julgamento humano constituí-se em uma parcela fundamental do ATC (TOMLIN et al., 1998). Este fato torna-se ainda mais grave se for observado o aumento de tráfego e a sobrecarga de trabalho humano dentro dos ATCs.

Atualmente toda a comunicação entre os aviões e os controles em terra é feita por voz, o que torna a comunicação deficiente e limitada, principalmente em função da velocidade e volume de informações a serem transmitidas.

Considerando-se que a taxa de crescimento do tráfego aéreo mundial nos próximos 15 anos deverá se situar entre 3% a 5% ao ano, pode-se afirmar que o sistema atual de controle do tráfego aéreo não está preparado para processar este volume crescente de tráfego, o que pode colocar a segurança do sistema aéreo em níveis não aceitáveis pela sociedade (TOMLIN et al., 2000).

Em função desses problemas, a comunidade internacional responsável pelo ATM vem estudando e implantando uma nova forma de controle do tráfego aéreo denominada CNS/ATM (*Communication, Navigation and Surveillance/Air Traffic Management*) (CIVIL, 1999).

O CNS/ATM trará como benefícios um espaçamento entre aeronaves e uma seqüência de chegada das mesmas nos aeroportos mais eficiente, através de maior automação dos sistemas. Outra função será a de melhorar também as decisões de suporte em situações conflitantes detectadas, com maior autonomia das aeronaves, permitindo rotas flexíveis em resposta ao tráfego e às condições climáticas adversas.

No CNS/ATM será utilizada comunicação via *links* de dados como formas de se intensificar e agilizar a comunicação vocal padrão atualmente utilizada. Haverá

transmissão de mensagens periódicas contendo informações pertinentes à navegação aérea, tais como posicionamento, identificação, latitude, altitude, velocidade em relação ao solo, entre outros parâmetros das aeronaves. Estes parâmetros são fundamentais em muitas funções, inclusive na Detecção de Conflitos entre aeronaves.

O ATM deverá permitir maior flexibilidade na operação de sistemas aéreos e uma melhor estratégia no gerenciamento do espaço aéreo por parte de pilotos, ATCs e companhias aéreas. O principal benefício será a adoção de rotas mais econômicas através da maior eficiência e colaboração entre as companhias aéreas, resultando em uma economia de centenas de milhões de dólares (LOZITO et al., 1997).

Da mesma forma que o estudo dos sistemas da Cia do Metropolitano de São Paulo, o estudo deste novo sistema de gerenciamento do tráfego aéreo, representa uma excelente aplicação para as linhas de pesquisa do autor descritas nesta tese, ou seja, os Sistemas Críticos e os Sistemas de Informação.

5.4. Propostas de Novos Trabalhos

Novos trabalhos devem ser realizados, visando dar continuidade às duas linhas de pesquisa aqui descritas, os Sistemas Críticos e os Sistemas de Informação, ou ainda a junção dos dois, ou seja, os Sistemas Computacionais de Segurança.

A maioria dos trabalhos está concentrada na área de software, que é o elemento dos Sistemas Computacionais de Segurança que merece maior atenção, tendo em vista que o hardware já apresenta um nível de maturidade superior, tanto no aspecto de projeto, quanto no aspecto de análise.

Dentre tais trabalhos, pode-se citar o problema do desenvolvimento de sistemas, nos quais é comum a alteração de requisitos, tendo em vista uma série de fatores, tais como mudança do ambiente, características não consideradas, e assim por diante. Tal fato também ocorre com os Sistemas Computacionais de Segurança. Desta forma, um trabalho que se coloca é o de definir métodos de projeto e de rastreabilidade, que permitam reduzir o impacto de mudança de requisitos no desenvolvimento e aceitação de Sistemas Computacionais de Segurança.

Outro trabalho a ser realizado refere-se à pesquisa por melhores técnicas ou ainda o aperfeiçoamento das técnicas atualmente existentes para a realização de atividades de Análise de Segurança do tipo quantitativo. O objetivo é a obtenção de métodos eficazes para a avaliação numérica de propriedades que permitam o estabelecimento de critérios, cujo propósito é o de avaliar a qualidade de implementação.

Dentre tais técnicas, merece atenção especial o estudo dos atributos de software mais indicados a sofrer esse processo de medição. O objetivo é que se possa afirmar que, a partir da medida de determinados atributos, um software apresente ou não a propriedade de Segurança Computacional. Um possível caminho a ser seguido consiste na decomposição de conceitos, ou seja, a partir de uma propriedade global de um software, decompô-la em propriedades locais, cuja verificação seja mais simples e direta.

Também é de grande importância o estudo e a definição de métodos de teste e sua respectiva cobertura sobre blocos do software, a respeito dos quais se conheçam apenas suas funcionalidades, ou seja, o código não é disponível. O objetivo é conseguir relacionar o grau de eventuais alterações efetuadas nesses blocos com a cobertura proporcionada pelos conjuntos de testes.

Nessa linha de testes de software, através de uma pesquisa detalhada, podem ser obtidos critérios que aumentem a capacidade de detecção de falhas presentes no software ou no hardware.

Outro trabalho a ser desenvolvido é a realização de um estudo comparativo das atuais técnicas de Segurança de Informação, tais como o reconhecimento por características biométricas, a utilização de senhas, de cartões de identificação, e assim por diante. Este estudo pode demonstrar a melhor adequação de um determinado método a certos tipos de aplicação, melhorando a eficiência da implementação.

A Análise de Segurança representa uma necessidade na certificação de Sistemas Computacionais de Segurança. Seguindo esta linha, propõe-se o estudo de linguagens e ambientes formais para a Análise de Segurança Computacional. Nessa

mesma linha de raciocínio, devem ser pesquisadas técnicas visuais para Análise de Segurança Computacional.

Na linha do software, devem ser feitas pesquisas a respeito de métodos formais de desenvolvimento de software utilizado em Sistemas Computacionais de Segurança.

Outro trabalho na linha de software refere-se à pesquisa sobre a modelagem e implementação de software, através da técnica de orientação a objetos para Sistemas Computacionais de Segurança, em especial os Sistemas Críticos, tendo em vista sua crescente utilização em outras áreas de desenvolvimento de software.

A utilização de programas comerciais de prateleira, em Sistemas Computacionais de Segurança, vem se demonstrando como uma opção cada vez mais considerada. Desta forma, é necessário que tenha continuidade a pesquisa sobre a utilização desse tipo de programas, incluindo sistemas operacionais, sistemas gerenciadores de bases de dados e os compiladores das linguagens utilizadas no software dos sistemas. Se puder ser comprovado que a utilização desses programas não traz insegurança aos sistemas, ou ainda se forem criados mecanismos que proporcionem proteção contra possíveis falhas nesses programas, se estará dando um grande passo na garantia da segurança de Sistemas Computacionais de Segurança. Desta forma, é importante o desenvolvimento de métodos, cuja finalidade seja a de certificar esses pacotes comerciais no desenvolvimento e implantação de Sistemas Computacionais de Segurança.

Na linha do hardware, devem ser melhor estudadas as atuais arquiteturas utilizadas, bem como podem vir a ser propostas novas arquiteturas, sempre visando a obtenção de melhores níveis de segurança.

Outro trabalho que deve ser realizado refere-se ao estudo de técnicas para aperfeiçoamento de diagnósticos de processadores. Estes se constituem no principal componente de um sistema computadorizado e a detecção de falhas em seu funcionamento é uma tarefa de extrema importância, de forma a permitir a realização de ações corretivas. Portanto, a pesquisa de técnicas e métodos que permitam a obtenção de diagnósticos mais precisos nos processadores é de vital importância.

Como praticamente todo sistema necessita, para sua operação, do elemento humano, é de extrema importância que se desenvolvam estudos para a avaliação da segurança da interação homem-computador em Sistemas Computacionais de Segurança. Este estudo deve compreender a análise da divisão de tarefas entre o ser humano e o computador, sempre visando uma operação segura.

Finalmente, inclui-se como atividade de pesquisa uma abordagem cultural, visando maior aperfeiçoamento da segurança, podendo envolver certificação de profissionais, de empresas e de cursos de treinamento na área de Segurança Computacional.

Estas novas propostas de pesquisas devem ser realizadas através da orientação a alunos de mestrado e de doutorado, bem como por intermédio de projetos de pesquisa e de extensão universitária, conforme tem sido a prática até aqui adotada.

Finalizando, pelas observações das duas linhas de pesquisa estudadas, ambas com trabalhos já concluídos, em fase de conclusão ou em andamento, pode-se verificar que há harmonia e integração entre os mesmos, demonstrando coerência nas diversas atividades até aqui realizadas.

6. CONSIDERAÇÕES FINAIS

Este capítulo está dividido em três itens. No primeiro item são apresentadas as principais conclusões e contribuições resultantes deste trabalho de Livre Docência, no sentido de se reunirem os conceitos básicos sobre Sistemas Críticos e Sistemas de Informação. Estas conclusões constituem-se em um resumo das conclusões apresentadas no capítulo 4.

No segundo item descrevem-se os futuros trabalhos a serem realizados, dando continuidade às duas grandes atividades aqui descritas. Esta seção é composta por um resumo dos futuros trabalhos já descritos no capítulo 5.

Finalmente, no terceiro item são apresentadas as considerações finais deste trabalho.

6.1. Conclusões e Contribuições

Uma das contribuições resultantes deste trabalho de Livre Docência é a reunião e apresentação dos principais conceitos relativos aos Sistemas Críticos e aos Sistemas de Informação, juntamente com os respectivos aspectos de Segurança Crítica e Segurança de Informação.

Outra grande contribuição refere-se ao estudo comparativo realizado entre esses dois tipos de sistemas, comparando-se cada um dos principais aspectos das duas áreas de aplicação.

Desta forma, foram apresentados os principais conceitos sobre segurança, os requisitos necessários, as principais formas de implementação, as formas de realização de atividades de análise de segurança, bem como as principais normas aplicáveis a cada área. Finalizando a apresentação dos conceitos, destacaram-se as principais aplicações, considerando-se cada área, ou seja, os Sistemas Críticos e os Sistemas de Informação.

Considerando-se cada um desses tópicos, foi esclarecido o significado, bem como foram colocadas as definições de diversos termos, cuja utilização apresenta algumas dificuldades em sua aplicação. Dentre tal nomenclatura destaca-se a proposição dos termos que reúnem os dois tipos de sistemas, ou seja, os Sistemas Computacionais de

Segurança, bem como a segurança dos dois tipos de sistemas, chamada de Segurança Computacional.

Este estudo foi feito com o objetivo de se verificar a possibilidade de integração, mesmo que parcial e considerando-se médio e longo prazos para a efetiva fusão, dos conceitos envolvidos em cada tipo de sistema. Neste item são resumidos os principais aspectos resultantes dessa comparação, apresentando-se seus pontos de destaque.

As considerações e conclusões apresentadas neste item descrevem a viabilidade de se considerar que os Sistemas de Informação venham a possuir, além de suas características peculiares, as características originárias de Sistemas Críticos. De forma similar, as considerações também vão no sentido de que os Sistemas Críticos venham a incorporar as características dos Sistemas de Informação, além se suas características próprias.

As comparações realizadas neste item têm como base as considerações realizadas no capítulo 4.

6.1.1. Conceito de Segurança

No aspecto referente ao conceito de segurança, a maior parte dos tópicos comentados leva a uma aproximação gradual dos conceitos de Segurança Crítica e Segurança de Informação, levando ao conceito de Segurança Computacional.

Um dos principais pontos levantados, no que se refere ao conceito de segurança está em que a Segurança de Informação e a Segurança Crítica são conceitos distintos, mas com tendência de aproximação pelo fato dos problemas de segurança em Sistemas de Informação também estarem sendo considerados como críticos.

Outra tendência indica que a Segurança de Informação venha, cada vez mais, a ser encarada como um pré-requisito para a Segurança Crítica.

As propriedades de confiabilidade e disponibilidade de Sistemas Críticos apresentam grandes analogias com as propriedades de integridade dos dados e de disponibilidade dos Sistemas de Informação. A confidencialidade é mais importante em Sistemas de

Informação, mas tem ganho importância em Sistemas Críticos. A propriedade da mantenabilidade é um fator importante no dois tipos de sistemas.

6.1.2. Cultura de Segurança

Considerando-se os diversos aspectos levantados, no tocante à cultura de segurança, pode-se afirmar que eles permitem levar a uma fusão dos Sistemas Críticos e de Informação, resultando na cultura de Segurança Computacional.

Há uma diferenciação feita, atualmente, no sentido de que nos Sistemas Críticos a preocupação maior está em falhas do próprio sistema, enquanto que nos Sistemas de Informação a preocupação se concentra em invasões aos sistemas. À medida que os Sistemas Críticos passarem a fazer utilização mais constante de redes de comunicação, estabelece-se a tendência de igualdade.

Um fator de igualdade refere-se à necessidade de uma cultura global de segurança nas organizações, incluindo-se treinamento e envolvimento da alta direção.

Outro fator de igualdade está no fato de que a política de segurança adotada deve ter ampla divulgação entre todos os envolvidos e que essa política seja flexível o suficiente para poder acomodar alterações que se façam necessárias.

A tecnologia utilizada é importante, mas representa apenas uma parcela de um plano de segurança, constituindo-se em outro aspecto de aproximação das culturas de segurança.

6.1.3. Requisitos de Segurança

Os requisitos de segurança dos Sistemas Críticos e dos Sistemas de Informação apresentam uma série de características comuns, levando-se a uma aproximação gradual dos mesmos, produzindo os Requisitos de Segurança Computacional. Dentre os aspectos comuns pode-se citar que alguns dos requisitos gerais mais importantes são pertinentes a ambos os tipos de sistemas. Dentre eles podem ser citados o desempenho, a disponibilidade, a confiabilidade, a usabilidade e a mantenabilidade. Esses requisitos gerais sofrem um processo de detalhamento, resultando nos requisitos específicos.

O objetivo dos requisitos de segurança é comum, ou seja, evitar condições perigosas ou de vulnerabilidade, prevenir a ocorrência de acidentes ou de invasões e minimizar conseqüências de eventuais condições de violação da segurança que venham a ocorrer.

6.1.4. Implementação

No tocante à implementação de Sistemas Críticos e Sistemas de Informação há predominância de aspectos distintos, principalmente no tocante ao software. Desta forma, uma aproximação dos conceitos a este respeito ainda está um pouco distante, embora possa vir a ocorrer.

Dentre os pontos em comum pode-se citar o uso constante de redundância de módulos. Por exemplo, é comum a existência de módulos de reserva para processadores, memórias, barramentos e discos rígidos, tanto em Sistemas Críticos, quanto em Sistemas de Informação. Através da redundância possibilita-se a obtenção de altos níveis de disponibilidade, menor probabilidade de se atingir estados considerados inseguros e melhora-se a qualidade da manutenção dos sistemas.

Outro aspecto concordante, na implementação de Sistema Críticos e Sistemas de Informação, está no fato de que se houver um núcleo básico responsável pela segurança em geral, torna-se mais fácil garantir que não haja falhas no sistema.

Seja qual for a aplicação de Sistemas de Informação ou de Sistemas Críticos, é de extrema importância a existência e realização de diagnósticos, de forma a se poder contar com mecanismos de detecção de falhas. De nada adianta ter toda uma arquitetura redundante, se não houver mecanismos que efetuem a detecção de falhas, permitindo ao sistema tomar as ações necessárias, indo desde a geração de alarmes até reconfigurações no sistema.

Pode-se dizer que a qualidade de implementação do hardware exerce influência em ambos os tipos de sistemas, pois a qualidade de módulos ou de componentes, a forma como são interconectados, bem como a maneira como são testados, exerce forte influência no funcionamento de tais sistemas.

Outro fator em comum está no nível de maturidade das instituições que desenvolvem os sistemas, o qual exerce grande influência na qualidade do desenvolvimento, tanto nos Sistemas Críticos, quanto nos Sistemas de Informação.

No entanto, há alguns aspectos divergentes. Um desses aspectos está no fato de que em certos casos, não é conveniente que se utilizem componentes de última geração, tendo em vista que nem sempre há a comprovação de um funcionamento plenamente correto, sendo necessário um certo tempo para a detecção de todas as falhas inerentes a um novo componente, principalmente aqueles de maior escala de integração.

Os cuidados tomados na implementação do software, ainda são distintos. Nos Sistemas de Informação utilizam-se, em grande quantidade, os programas comerciais, para os quais raramente há comprovação da ausência de falhas. Nos Sistemas Críticos, procura-se evitar a utilização desses tipos de programas, desenvolvendo-se as ferramentas de software de forma personalizada a cada aplicação.

Em Sistemas de Informação os circuitos utilizados em seu hardware são, em sua maioria, padronizados, havendo distinção com relação aos circuitos dos Sistemas Críticos, que quase sempre são projetados especialmente para cada aplicação.

6.1.5. Análise de Segurança

Ainda há muitos aspectos distintos na questão relativa à Análise de Segurança de Sistemas Críticos e Sistemas de Informação. Se houver uma maior aproximação das formas de implementação dos dois tipos de sistemas, a Análise de Segurança também irá sofrer um processo de uniformização, chegando-se ao conceito único de Análise de Segurança de Sistemas Computacionais.

O tipo de análise que se realiza é um pouco distinto. Nos Sistemas Críticos é necessária a realização de uma Análise de Segurança sobre todos os módulos de hardware utilizados no sistema, bem como sobre todos os programas de software, buscando-se verificar se há condições inseguras que possam vir a afetar o sistema.

No caso dos Sistemas de Informação, o foco principal está na possibilidade de perda da consistência dos dados e de invasões que possam resultar em roubo de

informações. O problema de invasões praticamente não existe, no momento, com relação aos Sistemas Críticos, mas sim a possibilidade de perda de consistência.

6.1.6. Normas

No aspecto referente às normas para Sistemas Críticos e para Sistemas de Informação, o problema está na diferenciação das conseqüências resultantes de disfunções de Sistemas Críticos e Sistemas de Informação. Se, de fato, ocorrer a unificação sobre a consideração dessas conseqüências, pode-se pensar na aproximação das normas, chegando-se às Normas para Sistemas Computacionais.

Atualmente há uma diferença de enfoque entre os dois tipos de sistemas, sendo que as normas para Sistemas Críticos estão voltadas à prevenção de estados inseguros e as normas para Sistemas de Informação visam a garantia da disponibilidade, sigilo e integridade das informações;

Outro aspecto a ser citado, é a existência de pressões por parte da população e de governos, no sentido de prover mecanismos que permitam uma fiscalização do projeto e implementação desses sistemas, sendo que as normas se constituem em um documento que pode ser utilizado com essa finalidade.

6.1.7. Aplicações

Vem ocorrendo uma aproximação gradual das considerações sobre as conseqüências decorrentes de disfunções de Sistemas Críticos e Sistemas de Informação. Na medida em que tais considerações levem a uma maior aproximação, também as aplicações poderão ser consideradas como unificadas, produzindo as Aplicações de Sistemas Computacionais.

Pode-se dizer que a principal distinção está no tipo de ação resultante da operação de cada sistema, que no caso dos Sistemas Críticos está centrada em ações físicas e no caso dos Sistemas de Informação o foco está em ações eletrônicas.

No entanto, cada vez mais as aplicações vêm tendo pontos em comum. É o caso de Sistemas Críticos que, com grande freqüência, vêm fazendo uso de bases de dados, cuja quantidade de dados vem apresentando tendência crescente.

Pode-se citar como fatores comuns, a necessidade de grande disponibilidade, da manutenção de consistência dos dados, bem como se evitar que se atinjam estados considerados inseguros.

6.2. Trabalhos Futuros

Os novos trabalhos a serem realizados estão incluídos nas áreas de sistemas, software, hardware, análise de segurança e recursos humanos, todos tendo como objetivo dar continuidade às duas linhas de pesquisa descritas, ou seja, os Sistemas Críticos e os Sistemas de Informação, reunidas no conceito de Sistemas Computacionais de Segurança.

Na área de Sistemas, deve ser realizado um trabalho de definição de métodos de projeto e de rastreabilidade, possibilitando a redução do impacto de mudança de requisitos no desenvolvimento e aceitação de Sistemas Computacionais de Segurança.

Na área de Análise de Segurança devem ser feitas pesquisas sobre técnicas para a realização de atividades de Análise de Segurança quantitativas, merecendo atenção o estudo dos atributos do software mais indicados a sofrer esse processo de medição.

Ainda na área de Análise de Segurança, outro trabalho a ser desenvolvido é a realização de um estudo comparativo das atuais técnicas de Segurança de Informação, tais como o reconhecimento por características biométricas, a utilização de senhas, de cartões de identificação, e assim por diante.

Nessa mesma linha da Análise de Segurança, propõe-se ainda o estudo de linguagens formais e ambientes formais para a Análise de Segurança Computacional. Nessa mesma linha de raciocínio, devem ser pesquisadas técnicas visuais para Análise de Segurança Computacional.

Na área de software, uma importante pesquisa a ser realizada é a de métodos formais de desenvolvimento de software a ser utilizado em Sistemas Computacionais.

Ainda na linha de software, um trabalho importante refere-se à pesquisa sobre a modelagem e implementação do software de Sistemas Computacionais de Segurança através da técnica de orientação a objetos.

É de grande importância que se dê continuidade à pesquisa sobre a utilização de programas comerciais, incluindo sistemas operacionais, sistemas gerenciadores de bases de dados e inclusive os compiladores das linguagens utilizadas. Se puder ser comprovado que a utilização desses programas não traz insegurança aos sistemas, ou ainda se forem criados mecanismos que proporcionem proteção contra possíveis falhas nesses programas, se estará dando um grande passo na garantia da segurança de Sistemas Computacionais de Segurança.

Na linha do hardware, devem ser melhor estudadas as atuais arquiteturas utilizadas, bem como podem ser propostas novas arquiteturas, sempre visando a obtenção de melhores níveis de segurança.

Continuando na linha do hardware, outro trabalho refere-se ao estudo de técnicas para aperfeiçoamento de diagnósticos de processadores, que são o principal componente de um sistema computadorizado.

No que se refere aos Recursos Humanos, praticamente todo Sistema Computacional de Segurança necessita de elementos humanos para sua operação, sendo de extrema importância que se desenvolvam estudos para a avaliação da segurança da interação homem-computador em Sistemas Computacionais de Segurança. Este estudo deve compreender a análise de tarefas a serem alocadas ao ser humano, sempre visando uma operação segura.

Finalmente, inclui-se como atividade de pesquisa uma abordagem cultural, visando maior aperfeiçoamento da segurança, podendo envolver certificação de profissionais, de empresas e de cursos de treinamento na área de Segurança Computacional.

6.3. Observações Finais

A questão da aproximação dos conceitos relativos aos Sistemas Críticos e aos Sistemas de Informação depende fundamentalmente da consideração das conseqüências de disfunções que venham a ocorrer. A tendência que vem se observando é que cada vez mais as perdas decorrentes em função de problemas nos Sistemas de Informação passem a ser considerados como apresentando conseqüências mais graves a seus usuários e à população de uma forma geral, passando a ser considerados como Sistemas Críticos.

Desta forma, pode-se dizer que a consideração da importância das perdas é que irá ditar o ritmo de adaptação dos Sistemas de Informação às características dos Sistemas Críticos. Da mesma forma, também à medida que os Sistemas Críticos passem a fazer uso mais constante de redes de comunicação e de bases de dados maiores, também haverá uma maior aproximação pelo lado dos Sistemas Críticos também passarem a ser vistos como Sistemas de Informação. Tal constatação conduz à fusão dos conceitos nos Sistemas de Segurança Computacional.

No momento, já está havendo uma aproximação entre esses dois tipos de aplicação, aproximação esta que deve se intensificar, conforme a tendência apontada ao longo desta tese vá se concretizando.

Por todas as definições, aplicações e exemplos descritos no decorrer deste trabalho, pode-se dizer que os conceitos aqui estabelecidos, ou seja, os Sistemas Computacionais de Segurança, bem como a Segurança Computacional vêm aos poucos se tornando uma realidade, conduzindo ao caminho de sua fusão.

Todos os trabalhos já concluídos ou em andamento apontados nesta tese, foram resultado de orientações a alunos de mestrado e de doutorado, bem como de projetos de pesquisa e de extensão universitária, conforme tem sido a prática até aqui adotada.

Finalizando, pelas observações das duas grandes atividades estudadas, pode-se verificar que há harmonia e integração entre as mesmas, demonstrando coerência nas diversas atividades até aqui realizadas pelo autor desta tese.

LISTA DE REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. Tecnologia da Informação – Código de Prática para a Gestão da Segurança de Informação. NBR ISO/IEC 17799. São Paulo, 2001.

ALMEIDA JR., J.R.; CAMARGO JR., J.B.; CUGNASCA, P.S. Metodologia de Análise de Segurança em Sistemas de Controle Computadorizados. In: CONGRESSO E EXPOSIÇÃO INTERNACIONAL DE AUTOMAÇÃO CONAI'2002, 10, São Paulo, SP, 5 a 18 de julho de 2002a. 1 CD-ROM.

ALMEIDA JR., J.R.; SHIMIZU, S.S.S.; CAMARGO JR., J.B.; SOUZA, B.J. Defensive Program for Safey-Critical Systems. In: APPLIED MATHEMATICS AND COMPUTER SCIENCE (AMCOS'2002). Rio de Janeiro, Brazil, October 21-24, 2002b. 1 CD-ROM.

ALMEIDA JR., J.R.; CAMARGO JR., J.B.; BASSETO, B.A.; CUNHA, R S.; PAZ, S. M. An Inspection List for Critical Software Analysis. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT – PSAM5, Osaka, Japão, November 27th to December 1st 2000. p.2369-2375.

ALMEIDA JR., J.R.; CAMARGO JR., J.B.; BASSETO, B.A.; CUNHA, R.S.; PAZ, S.M. Uma Lista de Inspeção para a Análise de Software Crítico. In: SSI'99 - SIMPÓSIO SOBRE SEGURANÇA EM INFORMÁTICA, São José dos Campos, SP, 14 a 16 de setembro de 1999. p.67-74.

ALMEIDA JR. J.R.; CAMARGO JR., J.B. Principais Aspectos da Segurança em Sistemas Utilizados em Áreas Críticas. In: CONAI - CONGRESSO NACIONAL DE AUTOMAÇÃO INDUSTRIAL, 7., São Paulo, SP, 25 a 27 de junho de 1996. p.114 - 120.

BERKELEY - SCHOOL OF INFORMATION MANAGEMENT & SYSTEMS, UNIVERSITY OF CALIFORNIA. How Much Information? Executive Summary. Apresenta informações estatísticas sobre a quantidade de informações existentes no mundo. Disponível em: <http://sims.berkeley.edu/research/projects/how-much-info/summary.html>. Aceso em 27 out. 2002.

BIFFL, S.; HALLING, M., Software Product Improvement with Inspection. In: EUROMICRO CONFERENCE 2000, 26., Maastricht, The Netherlands**,** 2000**.** vol.2, pp.262-269, 2000.

BRITTON, C. **IT Architectures and Middleware.** Essex, England, Addison Wesley, 2001. 336p.

BROOMFIELD, E.J.; CHUNG, P.W.H. Safety Assessment and the Software Requirements Specification. Reliability Engineering and System Safety, n.55, p.295-309, 1997.

BROWN, M.; LEVESON, N.G. Modeling Controller Tasks for Safety Analysis. In: WORKSHOP ON HUMAN ERROR AND SYSTEM DEVELOPMENT, Seattle, 1998. 10p.

BURNS, A.; WELLINGS, A. **Real-Time Systems and Programming Languages.** Essex, England: Addison Wesley, 1997. 611p.

BYRNES, F.C.; KUTNICK, D. **Securing Business Handbook**, Indianapolis: Addison Wesley, 2002. 237p.

CAMARGO JR., J.B.; CANZIAN, E.; ALMEIDA JR., J.R.; PAZ, S.M.; BASSETO, B.A.; Quantitative analysis methodologhy in safety-critical microprocessor applications. Reliability Engineering & System Safety, v.74, p.53-62, september-october 2001.

CAMARGO JR., J.B.; ALMEIDA JR., J.R. The Safety Analysis Case in the São Paulo Metro. In: SAFETY-CRITICAL SYSTEMS SYMPOSIUM, 7., Huntingdon, Reino Unido, 9 a 11 de fevereiro de 1999. p.100-110.

CARVALHO, L.A.V. **Data Mining**. São Paulo: Editora Érica, 2001, 237p.

CENELEC Comité Européen de Normalisation Electrotechnique Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), EN50126. 1999.

CENELEC Comité Européen de Normalisation Electrotechnique. Railway Applications – Safety Related Electronic Systems for Signalling - ENV 50129. . May 1998a.

CENELEC Comité Européen de Normalisation Electrotechnique Railway Applications – Software for Railway Control and Protection Systems -Final Draft, prEN 50128. July 1998b.

The CHANNEL Tunnel, a Safety Case**.** Channel Tunnel Publication, Langton Green, 1994. 294p.

CHENG, D.Y.; DEUTSCH, J.T.; DUTTON, R.W. "Defensive Programming" in the Rapid Development of a Parallel Scientific Program. IEEE Transactions on Computer-Aided Design, v.9, n.6, p.665-669, June 1990.

CIA DO METROPOLITANO DE SÃO PAULO – METRÔ. São Paulo. Apresenta descrição das atividades e de estatísticas do Metrô. Disponível em: http://www.metro.sp.gov.br. Acesso em: 02 Jan. 2003.

CIVIL Air Navigation Services Organization (CANSO) Group, Demystifying CNS/ATM, Report Final Version (June 1999). 105p.

CLARKE, R. Human Identification in Information Systems: Management Challenges and Public Policy Issues. Information. Technology and People. Vol.7, no.4, p.6-37. 1994

CORREA, P.L.P. **Diretrizes e Procedimentos para o Projeto de Bases de Dados Distribuídas.** 2002. 112p. Tese (Doutorado) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2002.

COURTRIGHT, W.V. **A Transactional Approach to Redundant Disk Array Implementation.** 1997. Dissertação (Mestrado) Department of Electrical and Computer Engineering, Pittsburgh, Carnegie Mellon Unversity, 1997.

CULLYER, J. The Technology of Safety and Security. Computer Bulletin, v.5, p.10-13, 1993.

DATE, C.J. **Introdução a Sistemas de Bancos de Dados.** Rio de Janeiro: Editora Campus, 2000. 803p.

DAPENA, P.R., Software Safety Certification: A Multidomain Problem. IEEE Software, p.31-38, July/August 1999.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação.** Rio de Janeiro: Axcel Books, 2000. 218p.

DROMEY, R.G. Cornering The Chimera. IEEE Software, p.33-43, Jan. 1996.

EAMES, D.P.; MOFFETT, J. The Integration of Safety and Security Requirements, In: SAFECOMP 99, Toulouse, France, September 1999. p.468-480.

ESSAMÉ, D.; ARLAT, J.; POWELL, D. Available Fail-Safe Systems. In: IEEE COMPUTER SOCIETY - WORKSHOP ON FUTURE TRENDS OF DISTRIBUTED COMPUTING SYSTEMS, 6., Tunis, Tunísia**,** 1997. p.176, 182.

FONSECA, A.J. **Arquitetura não Replicada de Hardware Aplicada em Sistemas de Controle com Requisitos de Segurança.** 2001. 126p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2001.

GANTI, V.; GEHRKE, J.; RAMAKRISHNAN, R. Mining Very Large Databases. Computer, p.38-45, august 1999.

GARRETT, C., APOSTOLAKIS, G., Context in the Risk Assessment of Digital Systems. Risk Analysis, vol. 19, no 1, p.23-32, 1999.

GERHART, S.; CRAIGEN, D.; RALSTON, T. Experience with Formal Methods in Critical Systems. IEEE Software, p.21-28, January 1994.

GHOSH, A. Addressing New Security and Privacy Challenges. IT Pro, p.10-11, May/June 2002.

GILB, T.; GRAHAM, D. **Software Inspection.** Essex, England**:** Addison Wesley, 1994.

HAGMAN, A.; GABLE, G. What Will Be of ERP? Project Report School of Information Systems, Queensland University of Technology, ITN 246. 2000.

HARMON, P.; ROSEN, M.; GUTTMAN, M. **Developing E-Business Systems and Architectures.** San Francisco: Morgan Kaufman and Publishers, 2001. 304p.

HATTON, L. Exploring the Role of Diagnosis in Software Failure. IEEE Software, p.34-39, July/August 2001.

HEDBERG, S.R. The Data Gold Hush. Byte, p.83-88, October 1995.

HOFMANN, H.F.; LEHNER, F. Requirements Engineering as a Success Factor in Software Projects. IEEE Software, p.58-66, July/August 2001.

HUNTER, J.M.D. **An Information Security Handbook**,Spriger Verlag, 2001. 226p.

HUSSENINY, A.A.; SABRI, Z.A.; ADAMS, S.K., RODRIGUEZ, R.J. Automation of nuclear power plants. Nuclear Technology, p.34-38, April, 1990.

IAEA - International Atomic Energy Agency. ANNUAL Report 2001, GC (46)/2. 2002a, Viena, Áustria. 162p.

IAEA - International Atomic Energy Agency. Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety Standard Series, No. NS-6-1.3, 2002b. 91p.

IBM – International Business Machine. Arriving at the upside of uptime: How people, process and technology work together to build high availability computing solutions for e-business. USA, 1999. 16p.

IEC International Eletrotechnical Commission. Information Technology – Security Techniques – Evaluation Criteria for IT Security, Parts 1 to 3. ISO/IEC 15408, Geneve, Switzeland. 91p. 1999.

IEC International Eletrotechnical Commission. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Part1 to 7, version 3.0, IEC 61508. 1997.

INMON, W. H. **Como Construir o Data Warehouse.** 3. ed. Rio de Janeiro**:** John Wiley & Sons, 1996. 388p.

JAFFE, M.S.; LEVESON, N.G.; HEIMDAHL, M.P.E.M.; BONNIE, E. Software requirements analysis for real time process control systems**.** IEEE Transactions on Software Engineering, v.17, n.3, p.241-258, Mar. 1991.

JIANG, H.; ELMAGRAMID, A.K. WVTDB – A Semantic Content-Based Video Database System on the World Wide Web. IEEE Transactions on Knowledge and Data Engineering, v.10, n.6, p.947-966, November/December 1998.

JOHNSON, B.W. **Design and Analysis of Fault Tolerant Digital Systems,** University of Virginia: Addison-Wesley Publishing Company, 1989. 584p.

KELLY, J.P.J.; MCVITTIE, T.I.; YAMAMOTO, W.I. Implementing design diversity to achieve fault tolerance. IEEE Software, v.8, n.4, p.61-71, July 1991.

KIMBALL, R. **Data Webhouse Construindo o Data Warehouse para a Web.** Rio de Janeiro: Editora Campus, 2000. 367p.

KIMBALL, R. **Data Warehouse Toolkit**. Rio de Janeiro: Makron Books, 1998. 388p.

KING, G. Best Security Practices: An Overview. In: NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE, 23., Baltimore, Maryland, 2000. 12p.

KITCHENHAM, B.; PELEEGER, S.L. Software Quality: The Elusive Target. IEEE Software, p.12-21, January 1996.

KNIGHT, J.C. Safety-Critical Systems: Challenges and Directions. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 24., Orlando, Florida**,** 2002. p. 547-550.

KOTONYA, G.; SOMMERVILLE, I. **Requirements Engineering – Process and Techniques**, New York: Jonh Wiley & Sons, 1998. 282p.

KRISHNAN, M.S., KELLNER, M.I. Measuring Process Consistency: Implications for Reducing Software Defects. IEEE Transactions on Software Engineering, v.25, n.6, p.800-815, November/December 1999.

KROENKE, D.M. **Database Processing Fundamentals, Design and Implementation.** New Jersey: Prentice Hall, 1998, 523p.

LACITY, M. Lessons in Global Information Technology Sourcing. Computer, p.26-33, August 2002.

LAUDON, K.C.; LAUDON, J.P. **Management Information Systems**, 6.ed. New Youk: Prentice Hall, 2002.

LEVESON, N.G. System Safety in Computer-Controlled Automotive Systems. In: SAE CONGRESS, LOCAL, March 2000, p.1-8.

LEVESON, N.G.; HEIMDAHL, M. New Approaches to Critical-Systems Survivability:Position Paper. In: INFORMATION SURVIVABILITY WORKSHOP, Orlando, Florida, 1998, paper 26.

LEVESON, N. G. **Safeware systems safety and computers.** New York: Addison Wesley Publishing Company, 1995. 680p.

LEVESON, N.G. High-Pressure Steam Engines and Computer Software. IEEE Computer, p.65-73, October 1994.

LI, Z.; YU, S.; LI, L. A New Safety Mechanism of Active Networks. In: INTERNATIONAL CONFERENCE ON INFO-TECH AND INFO-NET 2001, Beijing 2001. p.779-785.

LILI, E. Airports and CNS/ATM. Airport World, v.3, n.2, p.41-42, April-May, 1998.

LOZITO S., MCGANN A., MACKIONTOSK M.A.; CASHION, P. Free Flight and Self-Separation from Flight Deck Perspective. In: USA-EUROPE AIR TRAFFIC MANAGEMENT R&D SEMINAR, 1., Saclay, France, 1997.

MAHMOOD, A.; MCCLUSKEY E. J. Concurrent error detection using watchdog processors - A survey. IEEE Transaction on Computer. v.37. n. 2 p.160-174, Feb. 1988.

MAIWALD, E.; SIEGLEIM, W. **Security Planning & Disaster Recovery**, New Yourk: Mc Graw / Osborne, 2002. 299p.

MASSIGLIA, P.; MARCUS E. (Ed.) **The Resilient Enterprise – Recovering Information Services from Disasters.** Mountain View: Veritas Software Corporation, 2002. 527p.

MATHIASSEN, L.; HEJE, J.P.; NGWENYAMA, O. **Improving Software Organizations – From Principles to Practice**, 1.ed. MA, Addison-Wesley, 2001.

MCLEOD, R. **Management Information Systems**. New Jersey: Prentice Hall, 1995. 752p.

MILITARY Handbook. Reliability Predicition of Electronic Equipament-Department of Defense. – MIL-217F, Washington DC, 1990.

MOJDEHBAKHSH, R., TSAI, W. T., KIRANI, S., ELLIOTT, L. Retrofitting software safety in an implantable medical device**.** IEEE Software, pp. 41-50, Jan. 1994.

MONTAGUE, J. Safey Networks Begin go Emerge. Control Engineering, p.45-50, April 2002.

MOREIRA, N.S. **Segurança Mínima – Uma Visão Corporativa da Segurança de Informação.** Rio de Janeiro: Axcel Books, 2001. 240p.

MULUTINOVIC, V.; PATRICELLI F. (Ed.) **E-Business and E-Challenges.** IOS Press, 2002.

NASA - National Aeronautics and Space Administration. Software Safety. Technical Standard NASA-STD-8719.13A. September, 1997. 34p.

NATIONAL COORDINATION OFFICE FOR INFORMATION TECHNOLOGY RESEARCH AND DEVOLOPEMENT. Information Technology for the Twenty-First Century. 1999. Apresenta informações sobre a tecnologia da informação nos Estados Unidos. Disponível em: http://www.itrd.gov/ac/it2/initiative.pdf>. Acesso em: 02 Jan. 2003.

NIST – National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. National Institute of Standards Technology – NIST 800-30, Washington, 2001. 49p.

PATTERSON, D.A.; HENNESSY, J.L. **Computer Architecture: A Quantitative Aproach.** San Mateo, California: Morgan Kaufmann Publishing, 1990.

PIRIE, I.B. Software - How do we know it is safe? In: IEEE ASME RAILROAD CONFERENCE, 1999**.** p.122-129.

PORTER, A.; VOTTA, L. Comparing Detection Methods For Software Requirements Inspections: A Replication Using Professional Subjects. Empirical Software Engineering Journal, v.3, n.4, p.355-379, 1998.

PRICE WATERHOUSE COOPERS. Apresenta conceitos e estatísticas sobre segurança da informação. Disponível em: <http://www.betrusted.com>. Acesso em 22 Out. 2002.

REESE, J.D.; LEVESON, N.G. Software Deviation Analysis: A "Safeware" Technique. In: ANNUAL LOSS PREVENTION SYMPOSYUM, 31., Houston, Texas, 1997. p.1-14.

RTCA – Royal Technical Commission on Aviation. Software Considerations in Airborne Systems and Equipment Certification – RTCA DO-178B. 1998.

RUSSOM, P. The Right Architecture for e-Business Intelligence. Hurwitz Group Inc., July 2000. 10p.

SAEED, A.; LEMOS, R.; ANDERSON, T. The role of formal methods in the requirements analysis of safety-critical systems: a train set example. In IEEE INTERNATIONAL SYMPOSIUM ON FAULT TOLERANT COMPUTING, 21., Montreal, Canadá, 1991. p.478-85.

SAFEWARE ENGINEERING CORPORATION. Apresenta definições sobre a utilização de computadores em aplicações críticas quanto à segurança. Disponível em: http://www.safeware-eng.com/software-safety. Acesso em: 6 Out. 2002.

SCHULZE, M.; GIBSON, G. A.; KATZ, R.H.; PATTERSON, D.A. How Reliable is a RAID? In: SPRING COMPCON 89, San Francisco, CA, March 1, 1988. p.118-123.

SEAMAN, C.B. Qualitative Methods in Empirical Studies of Software Engineering. IEEE Transactions on Software Engineering, v.25, n.4, p.557-572, July/August 1999.

SERRA, A.P.G. **Proposta de Arquitetura Aberta de Central de Atendimento.** 2001. 140p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2001.

SHA, L. Using Simplicity to Control Complexity. IEEE Software, p.20-28, July/August 2001.

SIEWIOREK, D.P; SWARZ, R.S. **Reliable Computer Systems: Design and Evaluation**. 2.ed. Bedford, MA: Digital Press, 1992.

SIEWIOREK, D.P.; SWARZ, R.S. **The Theory and Practice of Reliable Systems Design**, New York: Digital Press, 1982.

SILBERSCHATZ, A.; KORTH, H.F.; SUDARSHAN, S. **Database System Concepts.** 4.ed., 2002, New York:McGraw Hill. 1064p.

SINGH, R. A Systematic Approach to Software Safety. In: ASIA PACIFIC SOFTWARE ENGINEERING CONFERENCE, 6., Takamatsu, Japão**,** 1999. p. 420-423.

STOREY, N. **Safety-Critical Computer Systems.** New York: Addison Wesley, 1996. 453p.

TEKLITZ, F.; McCARTHY, R.L. Analytical Customer Relationship Management, A White Paper from Sybase Inc, 1999.

THOMAS, S.W.; ALEXANDER, K.; GUTHRIE, K. Technology Choices for the JSTOR Online Archive. Computer, p.60-65, February 1999.

TOMLIN, C.; LYGEROS J., SASTRY S. S., A Game Theoretic Approach to Controller Design for Hybrid Systems. Proceedings of the IEEE, July 2000.

TOMLIN C. J., PAPPAS. G., GODBOLE D., SASTRY. S. Hybrid Control Models of Next Generation Air Traffic Management. Lecture Notes in Computer Science, v.1273, Springer Verlag. 1998.

TRIBBLE, A.C. Software Safety. IEEE Software, p.84-85, July/August 2002.

TSAI, W.T.; MOJDEHBAKHSH, R.; ZHU, F. Ensuring System and Software Reliability in Safety-Critical Systems. In: WORKSHOP ON APPLICATION SPECIFIC SOFTWARE ENGINEERING TECHNOLOGY - ASSET, Dallas, Texas**,** 1998. p. 1-6.

TSAI, W.T.; MOJDEHBAKHSH, R.; RAYADURGAM, S. Experience in Capturing Requirements for Safety-Critical Medical Devices in an Industrial Environment. In: WORKSHOP ON HIGH-ASSURANCE SYSTEMS ENGINEERING, Washington DC**,** 1997. p. 32-36.

TURBAN, E.; ARONSON., J.E. **Decision Support Systems and Intelligent Systems.** New Jersey: Prentice Hall, 1998. 890p.

VOAS, J. Roundtable – Fault Tolerance, IEEE Software, p.54-57, July/August 2001.

WALKER, A.J. Quality Management applied to the Development of a National Checklist for ISO 9001 Audits for Software. In: INTERNATIONAL SOFTWARE ENGINEERING STANDARDS SYMPOSIUM, 3., Walnut Creek, California**,** 1997. p.6-14.

WESTPHAL, C; BLAXTON, T. **Data Mining Solutions Methods**. New York: John Wiley, 1998.

WILLENSENS, P. **Modelagem Multidimensional de Dados para Sistemas de Data Warehousing.** 2002. 127p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2002.

WILLIAMS, L.G. Assessment of Safety-Critical Specifications. IEEE Software, p. 51-60, January 1994.

WILLIAMSON, G.F. Software Safety and Reliability. IEEE Potentials, v.16, n.4, p.32-36, October/November 1997.

WINTER CORPORATION. Apresenta informações estatísticas sobre a quantidade de informações existentes no mundo. Disponível em: http://www.wintercorp.com. Acesso em: 27 Nov. 2002.

WINTHER, R.; JOHNSEN, O.; GRAN, B.A. Security Assessments of Safety Critical Systems Using HAZOPs. In: SAFECOMP 2001, Budapest, Hungary, 2001. p.14-24.