UNIVERSIDADE FEDERAL DE ITAJUBÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Maurílio Pereira Coutinho

DETECÇÃO DE ATAQUES EM INFRA-ESTRUTURAS CRÍTICAS DE SISTEMAS ELÉTRICOS DE POTÊNCIA USANDO TÉCNICAS INTELIGENTES

Tese submetida ao Programa de Pós-Graduação em Engenharia Elétrica como parte dos requisitos para obtenção do Título de Doutor em Ciências em Engenharia Elétrica

Área de Concentração: Sistemas Elétricos de Potência

Orientador: Prof. Germano Lambert Torres
Co-orientador: Prof. Luiz Eduardo Borges da Silva

Outubro de 2007

Itajubá - MG

“The only way to discover the limits of the possible is to go beyond them into the impossible.
Arthur C. Clarke, "Technology and the Future" (Clarke's second law)
English physicist & science fiction author (1917 -)”

"Dedico este trabalho a minha querida esposa Marilia que soube, com sabedoria e paciência, atravessar comigo esta importante etapa de minha vida"

Agradecimentos

Aos meus pais, José (*in memoriam*) e Nina, pois sem eles este momento não teria existido;

Ao meu amigo, Prof. Horst Lazarek da TU-Dresden, grande responsável por este trabalho. Sua ajuda e apoio foram de fundamental importância para que este trabalho se concretizasse.

Aos meus Orientadores, Prof. Germano Lambert Torres e Luiz Eduardo Borges da Silva, que acreditaram e apoiaram este trabalho. Sem eles, com certeza, este trabalho não teria acontecido; Mais do que orientadores, eles ofereceram uma amizade que com certeza perdurará para sempre;

Aos meus amigos do GAIA, Carlos, Helga e Silvia, que me auxiliaram e encorajaram-me nos momentos finais deste trabalho;

A minha esposa e filhos, pela compreensão pelas longas horas ausentes;

SUMÁRIO

RESUMO

As infra-estruturas críticas desempenham funções importantes na sociedade atual. São exemplos destas infra-estruturas sistemas tais como redes de telecomunicações e de transporte, serviços de fornecimento de água e energia elétrica, sistema financeiro, dentre outras. Devido à interdependência estabelecida entre estas infra-estruturas, toda a sociedade está exposta às ameaças de segurança. Para protegê-las contra estas ameaças, os provedores destes serviços críticos necessitam manter os objetivos de segurança para suas redes de comunicação de dados. Os Sistemas SCADA constituem-se numa parte importante da infra-estrutura crítica do Sistema Elétrico de Potência e de outras infra-estruturas. Suas redes de comunicação de dados são potencialmente vulneráveis a ataques cibernéticos, necessitando de proteção contra uma variedade de ameaças, pois o item segurança não tem sido levado em conta em seus projetos. A diversidade e a falta de interoperabilidade nos protocolos de comunicação destas redes criam grandes obstáculos para qualquer organização que tente estabelecer uma rede de comunicação segura. A fim de melhorar a segurança dos sistemas SCADA, a técnica de detecção de anomalia tem sido utilizada para identificar valores corrompidos devido a ataques ou faltas provocadas de forma maliciosa. O objetivo deste trabalho é apresentar uma técnica alternativa para implementar detecção de anomalia para monitorar sistemas elétricos de potência. O problema é aqui abordado utilizando Técnicas Inteligentes.

ABSTRACT

Nowadays, Critical Infrastructure plays a fundamental role in our modern society. Telecommunication and transportation services, water and electricity supply, and banking and financial services are examples of such infrastructures. They expose the society to security threats. To safeguard against these threats, providers of Critical Infrastructure services also need to maintain the security objectives of their interdependent data networks. SCADA systems are an important part of the Electric Power System Critical Infrastructure. They require protection from a variety of threats and their networks are potentially vulnerable to cyber attacks because security has not been part of their design. The diversity and lack of interoperability in the communication protocols create obstacles for anyone attempting to establish a secure communication. In order to improve the security of SCADA systems, anomaly detection can be used to identify corrupted values caused by malicious attacks and faults. The aim of this work is to present an alternative technique for implementing anomaly detection to monitor Power Electric Systems. The problem is addressed here by the use of Intelligent Techniques.

Capítulo 1

INTRODUÇÃO

1.1 INFRA-ESTRUTURAS CRÍTICAS

As infra-estruturas críticas realizam serviços essenciais para a sociedade como um todo. São considerados serviços essenciais os serviços de comunicações, de transporte, de energia elétrica e do sistema financeiro, dentre outros. Sua operação contínua e confiável e o uso cada vez maior de Tecnologias da Informação (TI), tem tornado estas infra-estruturas críticas cada vez mais complexas e interdependentes, expondo a segurança da sociedade a vulnerabilidades e a ameaças. A proteção destes serviços relaciona-se com a proteção do espaço cibernético no nível mais fundamental devido a sua dependência no uso de redes computadores, roteadores, "switches", cabos de fibra-ótica e toda a infra-estrutura que garanta a sua funcionalidade.

A grande complexidade e a conseqüente interdependência tem levado a criação de uma abordagem de camadas que relacionam-se entre si e com outras infra-estruturas. São definidas 3 camadas: física, cibernética e de operação. Embora os problemas com segurança e proteção tradicionalmente existam nas camadas físicas e de operação, é na camada cibernética que residem atualmente as maiores preocupações dos provedores de serviços essenciais, devido principalmente ao aumento das vulnerabilidades presentes nesta camada.

Devido ao alcance e a influência destas infra-estruturas na vida da sociedade em todo o mundo globalizado, diversas iniciativas têm sido tomadas pelos setores públicos e privados, seja na criação de orientações a nível governamental, seja no estabelecimento de melhores práticas e padrões para a indústria como um todo.

1.2 INFRA-ESTRUTURAS CRÍTICAS DO SETOR ELÉTRICO

O setor de energia elétrica é constituído por várias instalações, tais como: unidades geradoras, linhas de transmissão, subestações de transmissão, subestações de distribuição, centros de controle de operação nacional, regional e local, unidades de terminal remotas (UTRs) / dispositivos eletrônicos inteligentes (IEDs – Intelligent Electronic Devices) e enlaces de comunicações. Estas instalações compõem a infra-estrutura crítica do setor elétrico. Os vários centros de controle que compõe esta infra-estrutura estão dispostos de forma hierárquica e contém cada um deles estações de trabalho que executam aplicações, tais como Sistemas de Gerenciamento de Energia (EMS – Energy Management Systems) e Banco de Dados, e estão conectadas através de Rede Local (LAN – Local Area Network). Estes Centros de Controle interagem com os Sistemas de Supervisão e Controle, chamados de sistemas SCADA (Surpervisory and Control Data Acquisition), que consistem de software especializado para realizar a interface com as unidades de hardware, UTRs e IEDs, as quais monitoram sensores e fazem a interface com os diversos dispositivos físicos do sistema elétrico, tais como os disjuntores, as chaves seccionadoras, os transformadores, os relés de proteção, etc. As UTRs e IEDs estão conectadas com os Centros de Controle via redes WAN (Wide Area Network). Estas conexões podem ser de propriedade da empresa de energia elétrica (privada) ou das concessionárias de serviços de telecomunicações (pública). Todas estas

instalações compõem o Sistema Interligado Nacional de Energia Elétrica. Este sistema é altamente interconectado e dinâmico, consistindo de diversas empresas, de natureza pública ou privada, que realizam os serviços de geração, transmissão, distribuição e comercialização de energia elétrica, constituindo o chamado mercado desregulamentado do setor elétrico. A figura 1.1 retirada de [56] apresenta um diagrama com os inter-relacionamentos destes diversos setores.

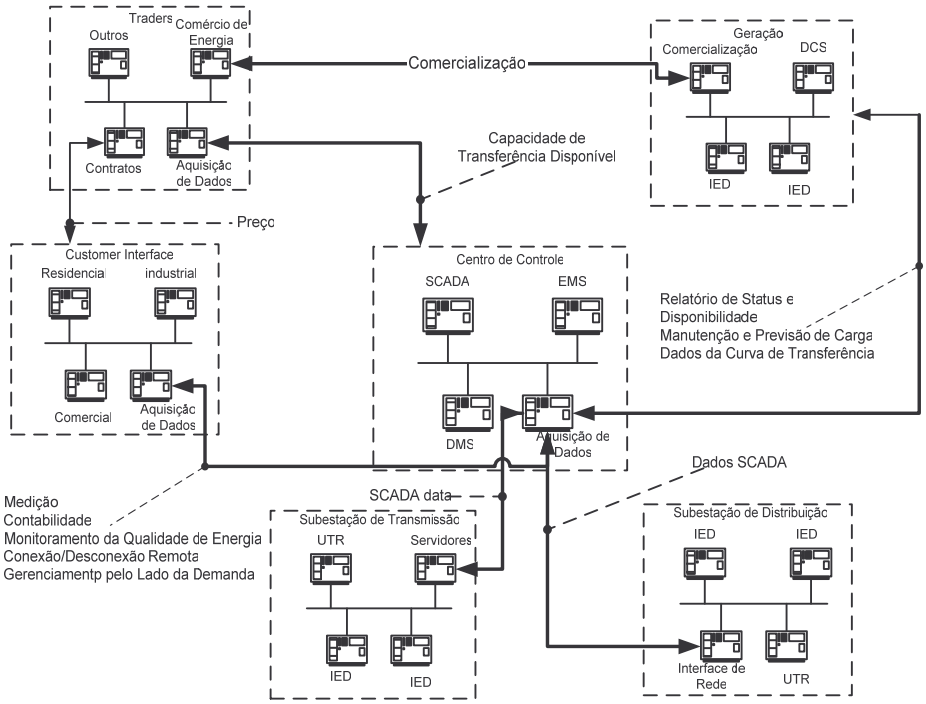


Figura - 1.1Modelo do Mercado de Energia Elétrica

Desta forma, estas instalações e aplicações realizam importantes funções para os serviços essenciais do sistema elétrico, fazendo parte da Infra-Estrutura Crítica Nacional e requerendo proteção especial contra uma variedade de ameaças, físicas ou cibernéticas.

1.3 DEFINIÇÃO DO PROBLEMA

A operação de um sistema elétrico de potência é intrinsecamente complexa devido ao alto grau de incerteza e ao grande número de variáveis envolvidas. As várias ações de supervisão e controle requisitam a presença de um operador, que deve ser capaz de responder eficientemente as mais diversas necessidades, através do tratamento de vários tipos de dados e informações. Estes dados são oriundos dos sistemas de medidas SCADA e de processos computacionais.

O aumento da base de dados do centro de controle nestes últimos anos deve-se, principalmente, ao fato do crescente uso das novas tecnologias de rede e de comunicações. Contudo isto tem tornado estes sistemas de controle cada vez mais vulneráveis a manipulação por invasores. A fim de melhorar a segurança dos sistemas de controle industrial, diversas medidas podem ser tomadas, como uso de "*firewalls*", controle de acesso, uso de criptografia, etc. Vários exemplos são encontrados na literatura sobre segurança em sistemas de controle industrial. Uma das soluções encontradas na linha do "*defense-in-depth*" é o uso de detectores de intrusão utilizados para identificar informações corrompidas por ataques e faltas de origem maliciosa.

O sistema de detecção de intrusão (IDS - Intrusion Detection Systems) é como um "alarme residencial anti-furto". Este tipo de dispositivo tem sido amplamente estudado nos últimos 20 anos e uma extensa bibliografia poder ser achada sobre o assunto. Estes sistemas podem ser caracterizados por diferentes propostas de monitoramento e análise. Com relação ao tipo de monitoramento eles podem ser empregados em 3 níveis: rede, "*host*" e aplicação. Com relação à análise dos eventos

existem 2 modelos básicos: detecção por abuso ou assinatura e detecção por anomalia. O primeiro tipo procura atividades na rede que sejam semelhantes ao conjunto de eventos que descrevem, de forma única, um tipo de ataque. É o método mais usado em sistemas comerciais. Os detectores de anomalias determinam ataques identificando o comportamento do sistema. Caso este comportamento fuja do que é considerado o perfil normal, um alarme é disparado. A premissa deste modelo se baseia na observação de que atacantes se comportam diferentemente dos usuários ditos normais e podem, então, ser detectados por sistemas que identificam estas diferenças. A maior diferença entre estes dois modelos está na capacidade de adaptação aos novos tipos de ataques: nos detectores de anomalias o comportamento é dinâmico, diferentemente dos sistemas por assinaturas. Existem atualmente diversos sistemas comerciais, de domínio público e aqueles resultantes de pesquisas.

Muitas pesquisas têm sido realizadas para implementar as métricas para análise em sistemas de detecção: por limites de operação ("*threshold*"), medidas estatísticas, medidas baseadas em regras e modelos utilizando técnicas de aprendizagem ("*machine learning*"), tais como técnicas de classificação, redes neurais, algoritmos genéticos e sistemas imunológicos. Apesar de haver ainda muita pesquisa sobre a eficácia do uso de tais técnicas alguns pontos vantajosos na sua utilização podem ser apontados: eficiência computacional, necessidade de poucos recursos de armazenagem e a capacidade de adaptar-se as novos dados (eventos). Além destes modelos pode-se apontar aqueles resultantes de pesquisas mais avançadas como o uso de "*Petri nets*", "*data fusion*" e representação por grafos.

1.4 SOLUÇÃO PROPOSTA

Muitas têm sido as soluções encontradas na literatura para implementação de detectores de anomalias utilizando-se técnicas inteligentes, pelos motivos já anteriormente expostos. Inclusive, algumas destas soluções se aplicam diretamente para o problema de proteção de infra-estruturas do sistema elétrico. A rede de um sistema elétrico de potência é controlada pela troca de sinais de controle entre os centros de controle e as UTRs, que por sua vez controlam disjuntores, transformadores, seccionadoras, etc. As tarefas de aquisição dos dados e do controle supervisório são executadas por meio dos sistemas SCADA. Os dados coletados por estes sistemas são, na maioria das vezes, incompletos e sujeitos a serem corrompidos. Pode-se definir dois modelos de detecção de intrusão por anomalia: (1) através da identificação de ataques que utilizam a infra-estrutura da rede de comunicação de dados e (2) através da modelagem do fluxo dos dados e das operações de controle em sistemas SCADA para detectar as anomalias produzidas por tentativas de causar prejuízos ao sistema, tais como mudança nos valores dos dados transmitidos, mudança dos sinais de controle, abertura dos disjuntores, fraudes, etc.

Uma das maiores dificuldades encontradas no monitoramento de sistemas elétricos de potência é a característica não linear de seu comportamento, obrigando o uso de métodos numéricos que em geral consomem tempo e recursos e não são indicados para um monitoramento on-line. Atualmente sistemas elétricos de potência utilizam uma aplicação chamada de Estimador de Estados, o qual é utilizado para lidar com estes problemas. Como o estimador de estados não consegue trabalhar bem com grande perda de dados, ele assume que sua informação sobre a rede é sempre correta. Esta é uma hipótese de risco, pois em geral existem erros de configuração bem como

sempre há a chance de que um atacante poderia estar mediando entre o centro de controle e o sistema elétrico. Este trabalho propõe e implementa uma aplicação para monitorar e proteger sistemas elétricos de potência no caso de ameaças cibernéticas usando técnicas inteligentes. A técnica proposta baseia-se na extração de conhecimento das bases de dados utilizando a Teoria dos Conjuntos Aproximados. Esta teoria foi desenvolvida por Zdzislaw Pawlak e pode ser classificada como mais uma poderosa técnica da Teoria do Conhecimento.

A proposta do trabalho é construir uma aplicação capaz de realizar o monitoramento on-line em subestações, coletando as medidas provenientes de UTRs e informando a ocorrência de eventos anômalos através de um detector de anomalias, como mostrado na Figura 1.2. Esta detecção pode-se dar em 2 etapas: projetar e implementar um classificador para detectar leituras erradas e corretas e projetar e implementar um classificador para o tipo de ataque ou erro introduzido. Em ambos os casos o detector deve disparar um alarme na presença de uma anormalidade.

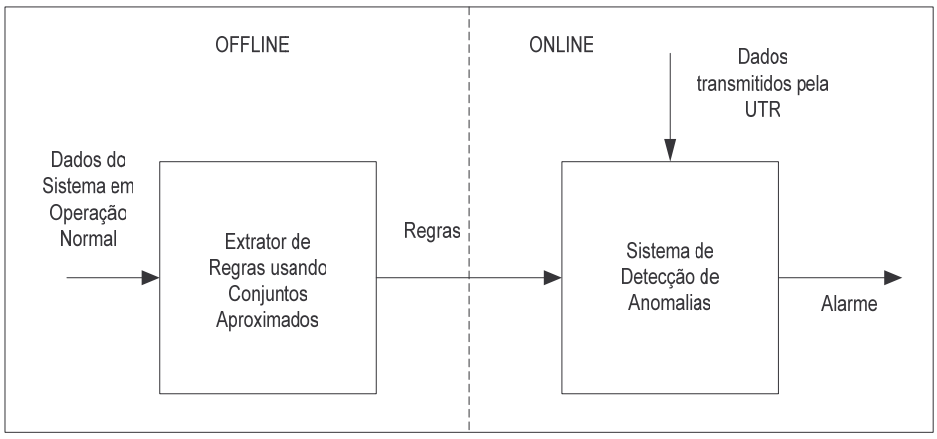


Figura 1.2 - Modelo do Detector de Anomalias Proposto

1.5 DESCRIÇÃO DOS CAPÍTULOS

Este documento divide-se em 9 capítulos:

- O capitulo 1 apresenta uma breve introdução ao problema de proteção de infra-estruturas críticas e propõe a implementação de um detector de intrusão por anomalias utilizando técnicas inteligentes para defender o sistema elétrico de potência de ameaças e ataques;
- O Capitulo 2 apresenta as definições e as diversas abordagens sobre Infra-Estruturas Críticas em termos mundiais e no Brasil. São analisadas as várias iniciativas para a proteção de infra-estruturas críticas, tais como normatizações, melhores práticas, etc.
- No Capitulo 3 são estudados as Infra-Estruturas Críticas para o Setor Elétrico nos EUA, União Européia e Brasil. Para cada caso são apresentadas as estruturas internas e as iniciativas para proteção do setor elétrico contra as ameaças cibernéticas;
- O Capitulo 4 introduz os principais conceitos de Redes de Computadores, tais como protocolos, redes TCP/IP e redes industriais;
- O Capítulo 5 introduz a questão de segurança da informação, abordando os aspectos dos ataques e dos mecanismos para segurança da informação. São abordados de forma especial os aspectos de segurança em sistemas de controle industrial;
- O Capitulo 6 apresenta as ameaças e as vulnerabilidades encontradas em sistemas elétricos de potência. É apresentada a estrutura de sistemas elétricos de potência e estudados cada um de seus componentes, procurando salientar as

suas vulnerabilidades. Sugere-se um grupo de melhores práticas para proteção de sistemas de controle industrial aplicados a Sistemas Elétricos de Potência e pesquisas realizadas na área de análise de vulnerabilidades;

- O Capitulo 7 introduz as técnicas para defender os sistemas de informação usando a técnica de detecção de intrusão. É feito um estudo sobre detectores de intrusão e referenciados os vários trabalhos publicados na área de detecção de intrusão nestes últimos 20 anos, salientando, principalmente, os algoritmos para implementar a análise de detecção;
- O Capítulo 8 estuda os aspectos de detecção de intrusão por anomalias em sistemas elétricos de potência. Faz-se uma revisão bibliográfica e apresentam-se alguns casos e as técnicas utilizadas para implementar o algoritmo de análise de detecção. É feita uma breve introdução da Teoria de Conjuntos Aproximados e apresentado o algoritmo de detecção de anomalias usando a Teoria de Conjuntos Aproximados;
- No Capitulo 9 apresenta-se a implementação do modelo de detecção de anomalias proposto e os resultados das simulações usando um sistema elétrico de 6 barras.
- No Capitulo 10 apresenta-se as conclusões do trabalho ora desenvolvido e sugestões para futuros trabalhos.

Capítulo 2

INFRA-ESTRUTURAS CRÍTICAS

As infra-estruturas críticas englobam em seu escopo diversos serviços essenciais para uma comunidade, estado e país. Serviços de comunicações, transporte, energia elétrica, fornecimento de água, serviços bancários representam alguns dos exemplos que podemos citar. A operação contínua e confiável destes serviços é critica para todos os setores da sociedade. Atualmente estas infra-estruturas estão fazendo uso cada vez maior de Tecnologias da Informação (TI) para melhorar a qualidade dos serviços prestados e fornecer novos serviços baseados em novas tecnologias aos seus clientes. Da mesma forma que o telégrafo revolucionou a infra-estrutura das comunicações no século 19, nos dias de hoje as redes de computadores e o uso de computadores cada vez mais poderosos estão revolucionando a sociedade da informação. Isto torna estas infra-estruturas críticas cada vez mais complexas e interdependentes expondo a sociedade a maiores vulnerabilidades e ameaças à sua segurança. A relação entre os componentes destes sistemas complexos torna-se imprevisível, como por exemplo, no caso de eventos de um sistema elétrico interligado que parecem ser insignificantes podem levar a uma falha em cascata, levando ao colapso o sistema regional ou mesmo o sistema nacional. Devido à interdependência com outras infra-estruturas este evento pode acarretar, ainda, a interrupção de serviços de emergência, fechamento de sistemas financeiros, etc.

As falhas de segurança são mais comuns em infra-estruturas que são integradas com redes interdependentes de comunicação de dados e de computadores. À medida que estas organizações desenvolvem novas tecnologias e processos para aumentar a velocidade nos quais os bens e serviços são produzidos, seus sistemas ficam cada vez mais expostos e vulneráveis. Com um computador e uma conexão a Internet, "hackers" podem remotamente acessar infra-estruturas críticas interconectadas e interdependentes, para interromper importantes serviços. Para se protegerem destes ataques cibernéticos, os provedores de serviços como energia elétrica, sistema financeiro, transportes, etc. devem procurar manter os objetivos de segurança, tais como, integridade, confidencialidade e disponibilidade para seus sistemas de informação, através da diferenciação, especialização, programação e padronização com o uso de melhores práticas e com a melhoria de seus sistemas de informação e comunicações.

2.1 PRINCIPAIS CONCEITOS

De acordo com as definições encontradas em [1, 2, 3, 4] tem-se que:

"Uma *infra-estrutura crítica* consiste nas facilidades, físicas ou virtuais, de tecnologias da informação, redes, serviços e instalações que, se interrompidas ou destruídas, causarão sérios impactos na proteção, na segurança e no bem-estar da economia e dos cidadãos, ou mesmo do efetivo funcionamento do governo."

E mais,

"Uma *infra-estrutura crítica de informações* consiste daquelas informações e facilidades de tecnologias de comunicações, redes, serviços e instalações que, se interrompidos ou destruídos, (1) causarão sérios impactos na proteção e na segurança do

bem-estar da econonomia e dos cidadãos, ou do efetivo funcionamento do governo, ou (2) causarão a interrupção do funcionamento de uma infra-estrutura crítica que ela suporta."

Entende-se por *produto ou serviço de uma infra-estrutura crítica* aquilo que é produzido pela mesma. *Setor crítico* compreende um conjunto de produtos e serviços da infra-estrutura crítica que são dirigidos como uma responsabilidade governamental e/ou privada comum. *Dependência* é uma ligação ou conexão entre dois produtos ou serviços, através do qual o estado de um influencia o outro. A dependência existe quando a entrada, criação, produção ou distribuição de um produto crítico ou serviço requer outro produto crítico ou serviço. *Intradependência* ou *interdependência* é a dependência mútua de produtos e serviços dentro da mesma infra-estrutura crítica ou entre infra-estruturas críticas, respectivamente. O aumento da interdependência tem levado a um crescimento das vulnerabilidades tornando os problemas ainda mais complexos.

O conjunto de serviços e produtos que pertencem a um setor evolui de acordo com as perspectivas históricas de organização e de responsabilidades dos governos. Portanto a atribuição de serviços e produtos a um determinado setor crítico depende de cada país, embora muitos deles reconheçam um conjunto mínimo comum de setores críticos. Os estudos apontados em [4] indicam os seguintes setores mais comumente encontrados em vários países como setores críticos:

- Energia
- Sistema Financeiro;
- Forças da Lei e da Segurança Pública;
- Saúde Pública;

- Telecomunicações
- Transportes e Logística; e
- Água Potável.

A proteção de todos estes setores relaciona-se com a proteção do espaço cibernético no nível fundamental devido a sua dependência no uso de redes computadores, roteadores, "switches", cabos de fibra-ótica e toda a infra-estrutura que garanta a sua funcionalidade.

O aumento da interdependência entre infra-estruturas críticas tem levado a um crescimento das vulnerabilidades tornando os problemas ainda mais complexos. Nos casos mais extremos, interrupções de serviços, modificação ou destruição inadequada de informação, podem ameaçar vidas e propriedades, possivelmente interrompendo atividades essenciais de governos e de corporações, resultando em riscos para a vida, para a liberdade e para propriedade [20].

2.2 ORGANIZAÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS EM CAMADAS

Em geral podemos dividir as infra-estruturas críticas em 3 camadas, conforme mostrado na Figura 2.1 [6]:

- **Camada Física:** Formada pela rede de dutos, linhas, fios, cabos, etc., que entregam os serviços essenciais. No domínio das tecnologias da informação esta camada consiste de roteadores, "switches", fios e cabos de cobre e fibra-ótica que transportam os dados; No domínio dos sistemas de energia elétrica a camada física constitui-se de diversas instalações e equipamentos, tais como geradores, linhas de transmissão, transformadores, disjuntores e chaves

seccionadoras, geradores, etc., que geram, transportam e distribuem a energia elétrica.

- **Camada Cibernética**: Composta de computadores, redes de sensores e coletores de dados que são utilizados para monitorar e controlar a camada física. No domínio das telecomunicações esta camada é utilizada para monitorar e controlar os vários roteadores e "switches" do sistema. Para o domínio de energia elétrica, esta camada coleta as informações acerca do fluxo de potência e estado dos equipamentos e transmite os sinais de controle do operador do sistema.

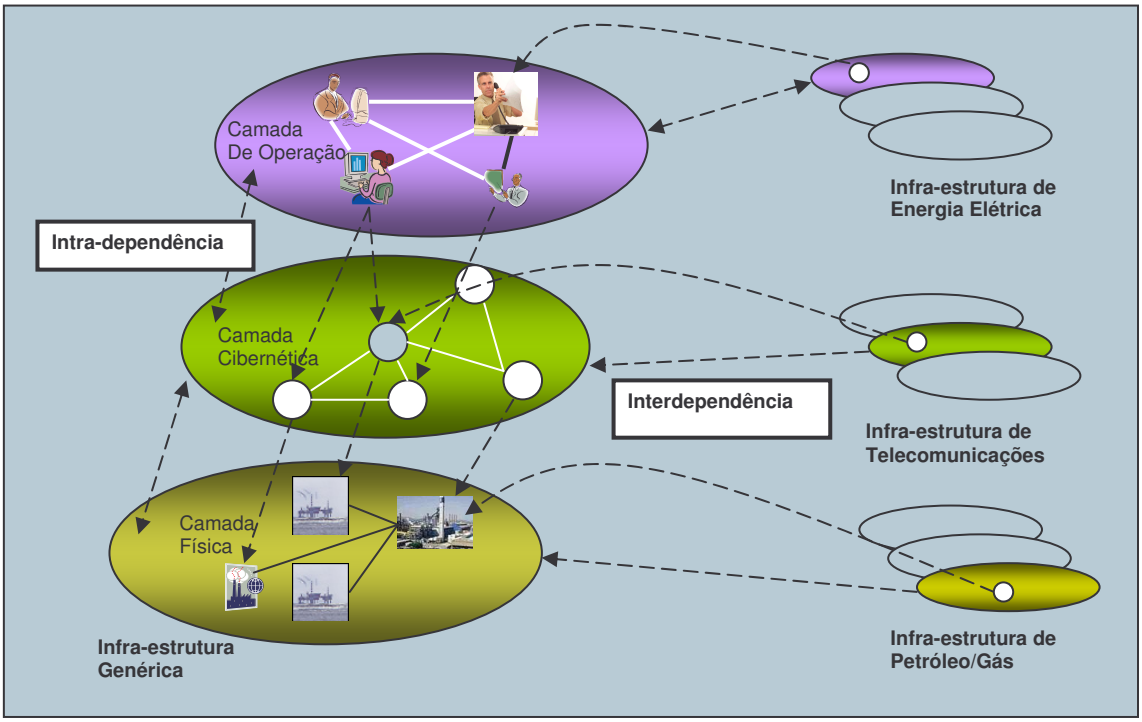


Figura 2.1 - Organização em Camadas e suas relações de interdependencia e intradependência.

- **Camada de Operação**: Todas as informações coletadas na camada Cibernética são passadas aos operadores, que as utilizarão para gerenciar as

camadas física e cibernética. Os processos organizacionais definidos para o gerenciamento, segurança e recuperação de falhas são partes desta camada.

Os acidentes e as falhas da camada física sempre fizeram parte da rotina diária da rede. Embora ocasionalmente, esta camada também tem sido vítima de ataques físicos. É ponto importante a salientar é que os operadores da Camada de Operação estão inevitavelmente sujeitos a erros, além de possuírem os conhecimentos necessários para também realizar ações maliciosas. Outro ponto importante a destacar é a possibilidade de atacantes ganharem acesso físico à salas de controle ou, ainda, que possam manipular os operadores através de "engenharia social". Embora estes problemas existam nos dias de hoje, é na camada cibernética que residem atualmente as maiores preocupações dos provedores de serviços, devido principalmente as vulnerabilidades presentes nesta camada e ao aumento de sua importancia nos dias de hoje.

O relatório preparado pelo "*Center for Digital Strategies at Tuck Scholl of Business at Dartmouth*" para o Banco Mundial, aponta os pontos chaves para a estruturação da segurança na camada cibernética [5]. A seguir são destacados aqueles pontos mais importantes:

- Minimização dos riscos em caso de ataques cibernéticos;
- Desenvolvimento de mecanismos para responder aos incidentes cibernéticos;
- Desenvolvimento de ferramentas contra ataques cibernéticos;
- Melhoria da qualidade do software de sistema e do software de aplicação;
- Coordenação e monitoramento das iniciativas de segurança cibernética entre os setores públicos e privados; e

- Coordenação internacional entre entidades dos setores público e privado que estejam envolvidas na estruturação da segurança cibernética.

Desta forma torna-se muito importante o desenvolvimento de metodologias para identificar o que é crítico em uma infra-estrutura e, portanto, identificar as ameaças, as vulnerabilidades e desenvolver recomendações de segurança [20].

2.3 Iniciativas para Proteção de Infra-estruturas Críticas no Mundo

Desde os ataques terroristas ao World Trade Center em 11 de Setembro de 2001, o terrorismo e a segurança interna tem sido uma grande prioridade na política governamental dos Estados Unidos da América. Exemplos podem ser vistos no documento "The National Strategy to Secure Cyberspace" [2] e na criação oficial do "Department of Homeland Security – DHS" em 2002 [7]. Muitas das iniciativas implementadas pelo DHS tem impactado diretamente a comunidade de Tecnologias da Informação como, por exemplo, a criação pelo DHS do "*DHS Daily Open Source Infrastructure Report*" (http://www.dhs.gov/xinfoshare/programs/editorial_0542.shtm). Este relatório diário é uma coletânea de informações relativas à questão de infra-estruturas críticas encontradas diariamente em diversas publicações. Outras medidas incluem a reorganização de agências governamentais, parceria público-privada, investimento em pesquisa e educação, bem como a adoção de novas tecnologias.

Atualmente além de organizações militares, várias corporações e instituições governamentais têm demonstrado interesse em criar metodologias para avaliar software e sistemas computacionais sob a perspectiva da segurança. Isto tem levado a criação de

vários critérios de avaliação. Este desenvolvimento é em geral financiado por governos com a parceria de grandes corporações. Uma destas metodologias de avaliação é o "*Trusted Computer Systema Evaluation Criteria*" (TCSEC) ou "*Orange Book*", criada em 1985 por iniciativa do Departamento de Defesa Norte Americano [8]. A versão canadense para este documento é o "*Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)*" que permitiu a harmonização entre os critérios canadenses e os critérios do TCSEC. Em 1990, por iniciativa da França, Alemanha, Holanda e Reino Unido o "*Information Technology Security Evaluation Criteria*" (ITSEC) [9] foi estabelecido. Este documento é uma harmonização das experiências de cada um dos países envolvidos buscando criar uma metodologia única de avaliação. A versão 1.2 deste documento foi a base para o desenvolvimento do "*Information Technology Security Evaluation Manual*" (ITSEM) [10].

Estes critérios de avaliação formaram a base para a criação conjunta pelos governos dos Estados Unidos da América, Reino Unido, França, Canadá e Comunidade Européia do "*Common Criteria for Information Technology Security Evaluation*" CC-ITSE [11]. O propósito deste documento foi coletar todas as propriedades desejáveis dos critérios existentes e criar um critério comum. Também conhecido como ISO/IEC 15408, o CC-ITSE é um meta-standard de critérios e construções utilizados para desenvolver especificações de segurança para suportar a avaliação de produtos e sistemas. Seu foco primário é melhorar a segurança em Tecnologias da Informação de sistemas de controle usado em indústrias de processos, incluindo concessionárias de energia elétrica, petróleo, água, esgoto, indústrias químicas, farmacêuticas, papel e celulose, mineração, com ênfase nas indústrias que compõem a Infra-Estrutura Crítica Nacional.

O "*Information Technology Baseline Protection Manual*" é uma iniciativa do "*Bundesamt für Sicherheit in der Informationteschnik*" (BSI) e recomenda uma série de melhores praticas de segurança para aplicações e sistemas de TI. Estas recomendações objetivam obter níveis de segurança que sejam apropriados e adequados e que possam servir com linha base para a proteção de sistemas sensíveis [12].

O "*British Columbia Institute of Technology*" (BCIT) mantém um banco de dados de incidentes de segurança industriais. Esta iniciativa tem por objetivo relatar incidentes de natureza de segurança cibernética que afetam sistemas de controle de processos industriais. São incluídos tanto eventos acidentais quanto deliberados [13].

O Dartmouth College mantém o I3P - "*The Institute for Information Infrastructure Protection*" (http://www.thei3p.org) que funciona como um consórcio de instituições acadêmicas, laboratórios governamentais e organizações sem fins lucrativos. Tem como objetivo agregar nacionalmente especialistas para identificar e mitigar ameaças à infra-estrutura de informações dos Estados Unidos da América. O I3P funciona como um laboratório virtual com a capacidade de organizar equipes e grupos de trabalho para dirigir pesquisas em relação às vulnerabilidades inerentes da infra-estrutura de informações.

O "*Process Control Security Requirements Forum*" (PCSRF) é um grupo de trabalho de indústrias composto por principalemente de profissionais de segurança para estimar vulnerabilidades e estabelecer estratégias apropriadas para o desenvolvimento de políticas para reduzir o risco da segurança de tecnologias da informação dentro das indústrias de controle de processos dos EUA. Como as vulnerabilidades são dependentes das arquiteturas das redes existentes, das políticas de TI e dos riscos associados com sistema de controle de processos em particular, o trabalho deste Fórum é identificá-las e documentá-las junto às indústrias representadas. Estas vulnerabilidades

serão utilizadas para o desenvolvimento de melhores práticas e de especificações de segurança [14]. Vulnerabilidades são, em geral, introduzidas em sistemas de controle de processos devido à falta de políticas.

O "*International Critical Information Infrastructure Protection (CIIP) Handbook*" é uma iniciativa do "*Eidgenössische Technische Hochschule Zürich (ETHZ)*" e outros parceiros que apresentam um inventário dos esforços de 20 países e 6 organizações internacionais na área de proteção de informações em infra-estruturas críticas [15]. Os dois volumes deste "*CIIP Handbook*" apresentam a grande diversidade dos modelos e das políticas existentes nos vários países e nas organizações relatadas. As principais questões que norteiam este trabalho são:

- Quais são os modelos de proteção de informações em infra-estruturas críticas existentes no mundo de hoje?
- Que métodos e modelos são utilizados nestes países para analisar e avaliar os vários aspectos destas infra-estruturas críticas?

Em função do relatório "*President's Commission on Critical Infrastructure Protection*" [16] solicitado pelo Presidente Clinton em 1997, o Ministro do Interior da Alemanha estabeleceu um grupo de trabalho em Infra-Estruturas Críticas (AG KRITIS) em 1997 com o objetivo de descrever:

- Possíveis cenários de ameaça para a Alemanha;
- Realizar análise de vulnerabilidades nos setores considerados críticos para a Alemanha;
- Fazer sugestões de contramedidas; e
- Criar um modelo para alertar sobre tais ameaças.

Os resultados deste grupo de trabalho foram de suma importância para as demais atividades das agências públicas alemãs [17].

Outro projeto de iniciativa européia é o CI^{2}RCO "*Critical Information Infrastructure Research Co-ordination*", cujo objetivo principal é criar e coordenar uma força tarefa européia para promover um amplo modelo europeu de coordenação de pesquisa e desenvolvimento na área de Proteção de Informações em Infra-Estruturas Críticas, estabelecendo uma "*European Research Area – ERA*" como parte da "*Information Society Technologies - IST*" [18].

2.4 Quadro Atual da Segurança Cibernética e Proteção de Infra-Estruturas Críticas no Brasil

O Brasil possui uma boa infra-estrutura de instituições envolvidas no desenvolvimento de políticas de segurança cibernética [5]. Segundo esta referência, a experiência brasileira ilustra bem o envolvimento dos setores públicos e privados da sociedade e suas relações em rede e que são essenciais para um quadro de segurança cibernética efetivo.

A seguir apresentamos alguns esforços no sentido de melhorar os níveis de segurança da informação no Brasil.

A segurança da informação no Brasil está dentro da jurisdição do Gabinete de Segurança Institucional – GSI (http://www.planalto.gov.br/gsi/index.htm), que responde diretamente ao Presidente da República. Suas atividades são definidas pelo Decreto No. 5.083 de 17 de Maio de 2004. O GSI não trabalha com os problemas de segurança da

Informação, mas sim através de outros órgãos, como o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Federal – CTIR-GOV (http://www.ctir.gov.br/), criado por portaria do GSI em 30 de junho de 2003, e o Comitê Gestor de Segurança da Informação - CGSI (http://www.planalto.gov.br/gsi/cgsi/), criado pelo Decreto Nº. 3505 de 13 de junho de 2000. Este decreto instituiu a política de segurança da informação nos órgãos e nas entidades da Administração Pública Federal.

O CTIR-GOV tem como finalidade o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal. Já o CGSI assessora a Secretária Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos no seu decreto de criação. A Figura 2.2 mostra as interações do CTIR-GOV.

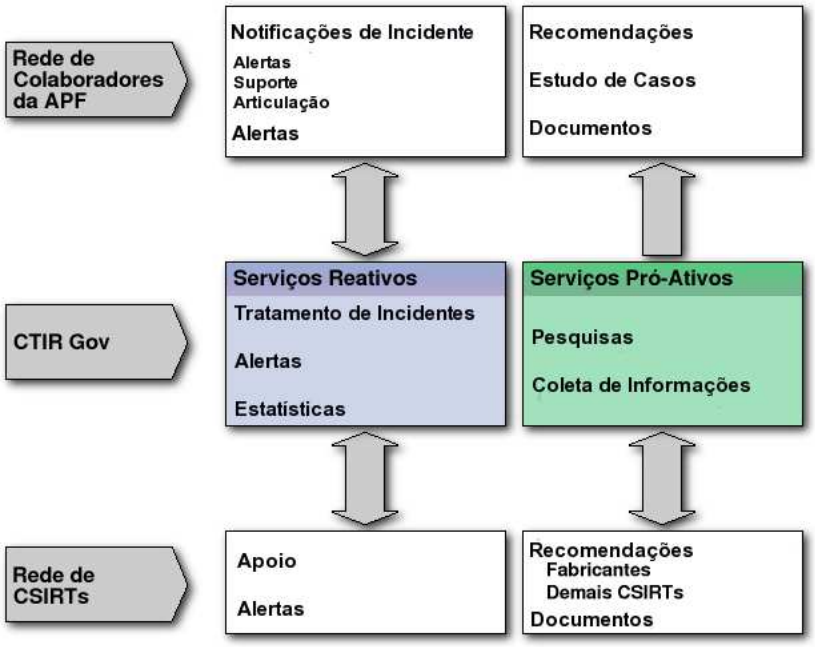


Figura 2.2 - Interações do CTIR-GOV (Fonte CERT.br).

Existe ainda uma rede de Grupos de Segurança e Resposta a Incidentes (CSIRTs). A Figura 2.3 apresenta a rede de CSIRTs no Brasil. O CERT.br (http://www.cert.br) é o grupo de resposta a incidentes de segurança para a Internet brasileira, mantido pelo NIC.br (http://nic.br), do Comitê Gestor da Internet no Brasil (http://www.cgi.br) .

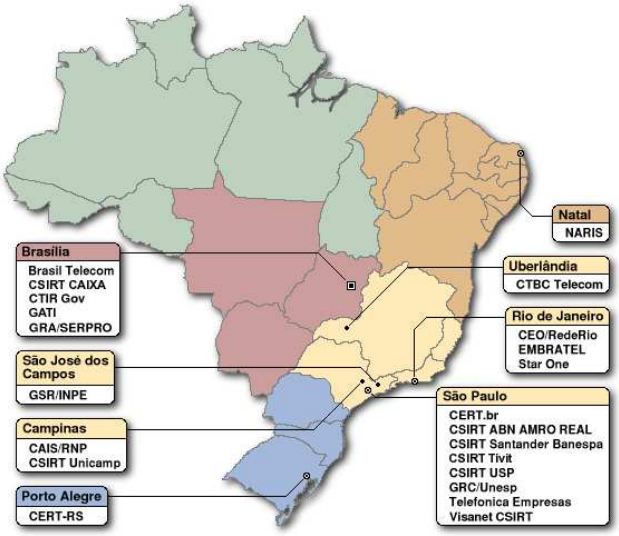


Figura 2.3 - Relação de CSIRTs no Brasil (Fonte: CERT.br).

Ele é responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O gráfico na Figura 2.4 apresenta o número de incidentes reportados ao CERT.br desde 1999. No ano de 2006 houve um sensível aumento nos incidentes reportados. Contudo, estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente foram notificados ao CERT.br. Segundo o CERT.br, a situação atual aponta para a existência de redes mal configuradas sendo abusadas para realização de atividades do crime organizado e por "*botnets*". Desta forma o alvo dos ataques está migrando para o usuário final.

Figura 2.4 - Total de Incidentes Reportados ao CERT.br por ano

(Fonte: http://cert.br/stats/).

O Centro de Atendimento a Incidentes de Segurança (http://www.rnp.br/cais) atua na detecção, resolução, prevenção de incidentes de segurança na Rede Nacional de Pesquisa (RNP2), além de criar, promover e divulgar práticas de segurança em Redes. Criado em 1997, o CAIS também divulga informações e alertas de segurança e participa de organismos internacionais na área.

Um importante ponto de discussão são os mecanismos para obter cooperação entre Governo e entidades privadas. Entre estas iniciativas podemos citar a realização anual da Conferência para Segurança para o Governo/ Seminário Brasileiro de Infra-estrutura Crítica – SEC GOV (http://www.secgov.com.br/), realizado pelo GSI-Gabinete de Segurança Institucional da Presidência da República. O objetivo desta Conferência é "pesquisar, consolidar, debater e gerar propostas de projetos e ações sobre os assuntos de maior relevância para: (1) Segurança da Infra-Estrutura Crítica do

Brasil, (2) Segurança da Informação e das Comunicações e (3) Terrorismo". Este evento envolve profissionais do governo, bem como das Agências Reguladoras e de entidades privadas. Na segunda Edição desta Conferência, SEC GOV/2006, realizada em 27/11 a 28/11 de 2006, foram discutidas questões de interoperabilidade, segurança lógica, Tratamento de Incidentes e segurança física para os seguintes setores críticos: Segurança Pública, Energia, Finanças, Transporte, Água, Saúde, Telecomunicações e Terrorismo. O SecGov 2006 representou mais um passo para a criação de um fórum permanente para gerenciamento e investimento na infra-estrutura brasileira, consolidando o processo de discussão e proposição de políticas de ação iniciado durante a Conferência de Segurança da Organização dos Estados Americanos em Setembro de 2005. Para subsidiar as discussões desta edição do SECGOV, foi publicado o "Livro Verde da Infra-estrutura Crítica do Brasil" (http://www.secgov.com.br/Livro_Verde.aspx), que levantou algumas das principais discussões e problemas em cada um dos setores críticos apontados e a visão de vários responsáveis por este planejamento dentro do governo brasileiro.

As referências [19] e [20] apresentam metodologias para proteger infra-estruturas críticas no Brasil, em especial a infra-estrutura de telecomunicações. Em [19] são discutidos as necessidades e desafios para a definição de uma metodologia para proteção da infra-estrutura crítica de Telecomunicações. A referência [20] apresenta a necessidade de proteção de infra-estruturas críticas, realiza uma contextualização do Brasil e apresenta a Metodologia para Identificação de Infra-estruturas Críticas, MI^2C, e sua aplicação para Identificação e Análise da Infra-estrutura Crítica de Telecomunicações no Brasil a ser protegida de agentes maliciosos. A metodologia

apresentada é uma das fundamentais para a proteção de diferentes infra-estruturas, tais como energia, transportes ou telecomunicações.

Além do Decreto No. 3505 que ainda não foi adequadamente implementado, não existem leis específicas criadas para cuidar dos problemas de segurança da informação. Este decreto estabeleceu dentre outras coisas:

- Classificação e Tratamento da Informação;
- Pesquisa e Tecnologias para apoio a Defesa Nacional;
- Atestar e certificar produtos e serviços;
- Garantir a interoperabilidade de sistemas;
- Estabelecer regras e padrões relacionados à Criptografia; e
- Sistemas que garantam a confidencialidade, disponibilidade e integridade da informação

No que diz respeito a padrões de criptografia o CGSI apresentou proposta que se constituiu no Decreto No. 3587, de 5 de setembro de 2000, estabelecendo normas para implantação da Infra-estrutura de Chaves Públicas (PKI) do Poder Executivo Federal – ICP-GOV.

O Decreto No. 3505 também estabeleceu o Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações – CEPESC (http://ww.abin.gov.br/abin/cepesc_abertura.jsp). Este Centro fornece suporte técnico em segurança da informação a organizações estatais e promove a pesquisa científica e tecnológica aplicada a projetos relacionados à segurança das comunicações. Além disso, assessora os dirigentes do Estado brasileiro nas políticas e ações que envolvam

utilização de recursos criptográficos. Este centro é parte integrante da estrutura do Departamento de Tecnologia da Agência Brasileira de Inteligência (ABIN).

Em 24 de março de 2004, o governo federal baixou Portaria Normativa 333, do Ministério da Defesa, que instituiu a Política de Guerra Eletrônica de Defesa. O artigo 2° desta portaria mostra que a nova política do governo federal tem o objetivo de orientar a chamada "Guerra Eletrônica" no âmbito das Forças Armadas para atender às necessidades da defesa nacional.

Capítulo 3

INFRA-ESTRUTURA CRÍTICA DE ENERGIA ELÉTRICA

A indústria de energia elétrica pode ser considerada uma das infra-estruturas críticas mais sensíveis, pois incorpora objetivos potencialmente fundamentais para o correto funcionamento de outras infra-estruturas. A despeito da existência de recursos e procedimentos de retaguarda para a continuidade das operações, se o setor de energia elétrica entra em colapso, comunicações são prejudicadas, trens param, aviões deverão ficar em terra, e a economia pode ser seriamente prejudicada. Diferentemente de outros tipos de energia, energia elétrica não pode ser armazenada; portanto, as interrupções no fornecimento de energia elétrica produzem efeitos imediatos.

Dezenas de casos tem havido onde sistemas de controle – em sistemas elétricos, água, esgoto, petróleo, gás e indústrias de papel e celulose - têm sido impactados intencionalmente ou não intencionalmente por meios eletrônicos, de acordo com operadores e especialistas da indústria. Além disso, atacantes "*online*" estão buscando utilizar o sistema de informações corporativo das companhias de energia elétrica como porta de entrada para os sistemas de controle. Estas informações mostram como o setor de energia elétrica pode ser vulnerável a ataques cibernéticos de terroristas, "*hackers*", nações hostis, etc.

Não são claras quais as conseqüências que poderiam advir de um ataque cibernético contra sistemas de controle no setor de energia elétrica. Contudo, através dos relatos dos acidentes e erros que levaram a pequenas interrupções ou falhas, locais ou regionais, podemos concluir que é relativamente fácil para um "*hacker*" experiente perpetrar tais ataques. Ataques coordenados contra sistemas regionais de energia elétrica também são passíveis de ocorrer, tendo em vista as atuais vulnerabilidades encontradas nestes sistemas.

3.1 ESTRUTURA DO SISTEMA ELÉTRICO

O Sistema Interligado Nacional de Energia Elétrica (SIN) é altamente interconectado e dinâmico, consistindo de várias empresas concessionárias privadas ou públicas. E mais, este sistema tem uma característica hierárquica, sendo subdivididos em sistemas regionais, como mostrado na Figura 3.1. Além disso, existe a subdivisão do setor em geração, transmissão, distribuição e o mercado comercialização de energia elétrica.

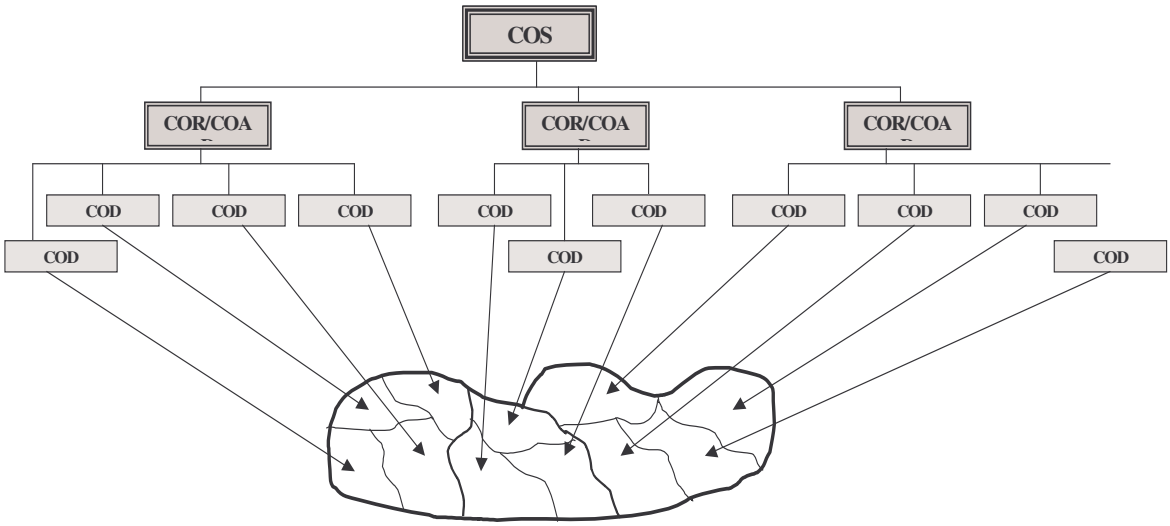


Figura 3.1 - Sistema Hierárquico de Controle [134].

O setor de energia elétrica é constituído por várias instalações, tais como [21]:

- Unidades Geradoras;
- Linhas de Transmissão;
- Subestações de Transmissão;
- Subestações de Distribuição;
- Centros de Controle de Operação Nacional, Regional e Local;
- Unidades de Terminal Remotas (UTRs) / Dispositivos Eletrônicos Inteligentes (IEDs); e
- Enlaces de Comunicações.

Os Centros de Controle de Operação Nacional, Regional e Local abrigam os Sistemas de Controle e Gerenciamento de Energia das empresas concessionárias e do Operador Nacional do Sistema Interligado, como mostrado na Figura 3.2.

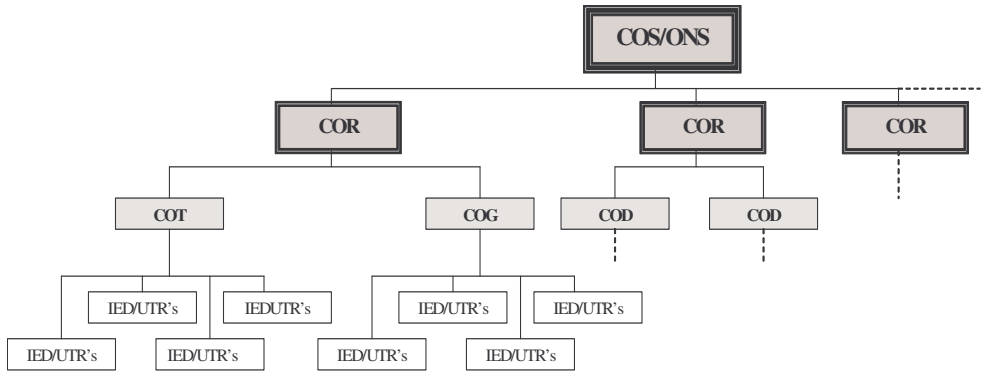


Figura 3.2 - Organização Hierárquica dos Centros de Operações e Instalações [134].

Estes monitoram os dados obtidos pelas UTRs e pelos Sistemas de Controle e Operação das Subestações (Transmissão e Distribuição) para garantir que o sistema está

funcionando adequadamente. Os Centros de Controle e Operação também despacham mensagens de controle para as Unidades Geradoras e Subestações para regular o fluxo de potência, como mostrado na Figura 3.3.

Sistemas Computacionais para Controle que permitem aos operadores a regulação do fluxo de potência (geração, transmissão e distribuição) são chamados de Sistemas de Gerenciamento de Energia Elétrica (em inglês, EPMS ou simplesmente EMS). Já os sistemas de controle utilizados para monitoramento da segurança, confiabilidade e proteção do sistema elétrico são chamados de Sistemas de Controle Supervisório e Aquisição de Dados (em inglês, SCADA – "Supervisory Control and Data Acquisition"). Em geral, os operadores e administradores do sistema utilizam o EPMS, enquanto que os engenheiros de proteção e automação/integração utilizam e são responsáveis pelos Sistemas SCADA.

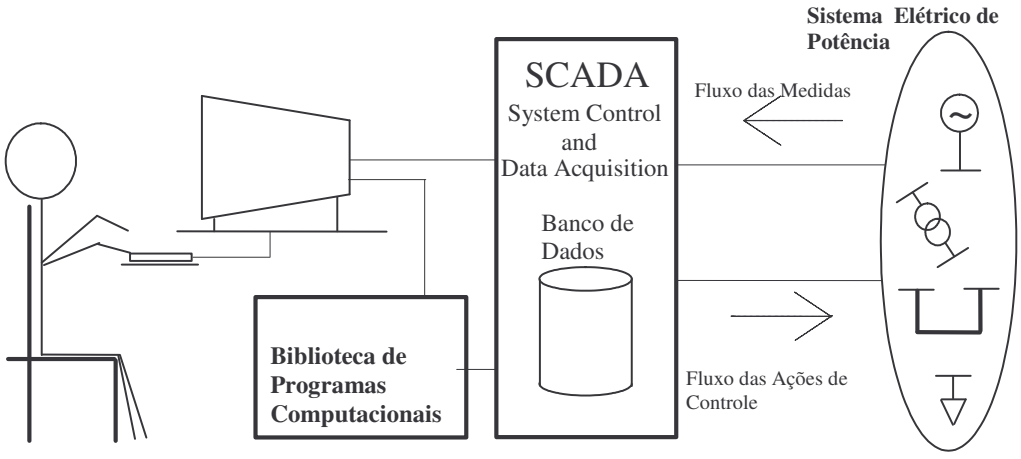


Figura 3.3 - Sistema de controle e gerenciamento de energia / Sistema SCADA [135].

Os sistemas de controle contêm computadores e aplicações que realizam importantes funções para os serviços essenciais do sistema elétrico. Como tal, eles

fazem parte da Infra-Estrutura Crítica Nacional e requerem proteção contra uma variedade de ameaças. Como estes sistemas se baseiam em redes e em hardware proprietário, eles têm sido erroneamente considerados imunes a ataques cibernéticos e a segurança. Este é um tópico desconsiderado no projeto de tais sistemas. Se forem incluídos no projeto, são muito limitados, por diversas questões, mas, principalmente, por razões econômicas. Isto torna estes sistemas potencialmente vulneráveis. A interrupção de serviços, negação de serviço distribuída, redirecionamento de processos, ou mesmo manipulação de dados operacionais podem levar a desestabilização de infra-estruturas críticas. Ataques cibernéticos em sistemas de produção e distribuição de energia elétrica colocam em risco o bem estar e a segurança pública, assim como podem causar sérios danos ambientais. A introdução de Tecnologias da Informação (TI) baseadas em Internet e as novas estratégias de integração de negócios juntamente com o pouco conhecimento em segurança de TI neste tipo de ambiente, tem tornado ainda mais os sistemas de controle de processos industriais vulneráveis a ataques cibernéticos. A referência [22] apresenta informações de incidentes coletados pelo "*Industrial Security Incident Database – ISID*" do "*British Columbia Institute of Technology*" e descreve vários eventos que impactaram diretamente sistemas de controle de processo até os dias de hoje, bem como discute as lições aprendidas destes eventos (http://www.bcit.ca/appliedresearch/security/services.shtml).

A tendência de evolução dos Centros de Controle e Operação tem sido na direção da utilização do acesso remoto, usando-se os meios de comunicação público, Internet e Tecnologia Wireless, como mostrado na Figura 3.4. Em função das vantagens econômicas para a realização das funções de gerenciamento e manutenção, este aumento de conectividade tem levado a uma maior automatização das subestações de

transmissão e distribuição e, por conseguinte, um aumento das conexões entre os sistemas de monitoramento e os sistemas de informação corporativos. Esta tendência traz consigo os riscos de ataques cibernéticos perpetrados por "hackers" e/ou terroristas. Invasões podem produzir efeitos desastrosos se dispositivos de controle forem maliciosamente manipulados. A fim de proteger o sistema elétrico contra este tipo de ameaças, necessário se faz identificar as vulnerabilidades para, então, torná-lo mais robusto ("*harden*") contra invasores e atacantes.

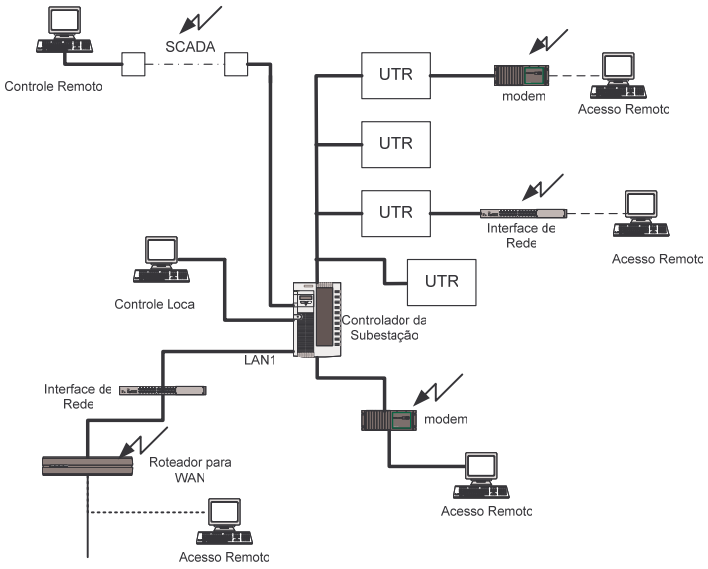


Figura 3.4 - Acessos remotos encontrados na infra-estrutura de Energia Elétrica [23].

Atualmente, o grande desafio para a indústria de energia elétrica está na integração da diversidade de equipamentos e protocolos utilizados na comunicação e no controle de sistemas elétricos. Exemplos de protocolos encontrados em sistemas de controle em subestações incluem protocolos proprietários, protocolos Ethernet e FastEthernet, EIA232/485, UCA ("Utility Comunication Architecture") e UCA2, ControlNet, TCP/IP, V.32, WAP, WEP, DNP3, IEC60870, IEC61850, Modbus, Profibus, Fieldbus, entre outros. Estes protocolos são utilizados para conectar os

sensores e os Dispositivos Eletrônicos Inteligentes (IEDs), a equipamentos de controle, tais como Controladores Lógicos Programáveis (CLPs), Unidade de Terminal Remota (UTR), processadores de comunicação, PCs locais e dispositivos do sistema SCADA. A Figura 3.5 mostra um exemplo desta estrutura.

A diversidade e a falta de interoperabilidade destes protocolos de comunicação criam obstáculos para qualquer intenção de estabelecimento de um enlace seguro de comunicação entre subestações. Além disso, existe também uma variedade de meios de comunicação utilizados para acessar estes equipamentos e sistemas. É comum encontrarmos telefonia pública, rede "wireless", enlace de microondas, cabos de fibra ótica, conexões a rede Internet nas interconexões das subestações com centros de controle [23].

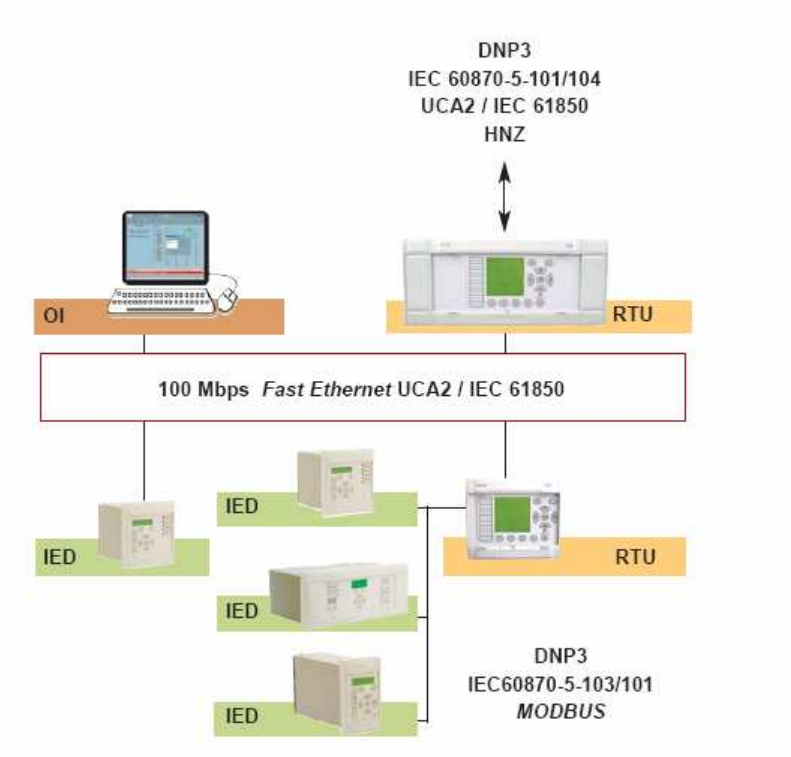


Figura 3.5 - Arquitetura Típica de um Sistema SCADA (Fonte: Areva T&D).

3.2 INFRA-ESTRUTURA DE ENERGIA ELÉTRICA DOS ESTADOS UNIDOS DA AMÉRICA

A infra-estrutura de energia elétrica dos Estados Unidos da América, conforme mostrado na Figura 3.6, inclui uma rede de linhas de transmissão de grande comprimento e espalhadas por todo o país que transportam energia elétrica de região para região, bem como linhas de distribuição local que transportam energia elétrica para empresas e consumidores domésticos. A energia elétrica origina-se em unidades geradoras alimentadas principalmente por carvão, energia nuclear, gás natural, água, e, em menor escala, por petróleo. Carvão, gás natural e petróleo dependem, ainda, da existência de uma infra-estrutura de transporte para fornecer o combustível necessário para produção de energia elétrica.

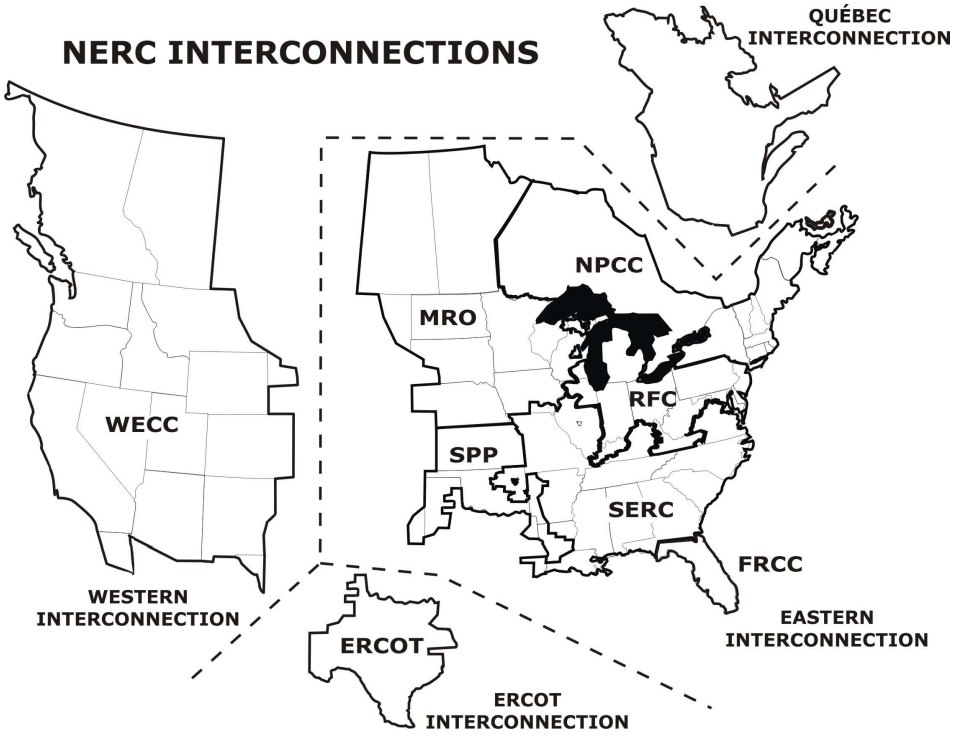


Figura 3.6 - Infra-estrutura de energia elétrica dos EUA (Fonte: http://www.nerc.com).

As mudanças ocorridas no setor elétrico norte americano afetaram o modo de operação de sua infra-estrutura de energia elétrica nas últimas décadas. A reestruturação do modelo verticalizado das empresas concessionárias de energia elétrica separou geração, transmissão e distribuição em empresas distintas. Para facilitar a competição ao nível do mercado atacadista de energia elétrica, em 1996 o "Federal Energy Regulatory Commission – FERC" (http://www.ferc.gov/) solicitou que as concessionárias dos serviços de transmissão abrissem suas ofertas de transmissão ao mercado de energia, para ofertar seus sistemas de transmissão de forma livre e não discriminatória para outras concessionárias e produtores independentes de energia. No nível do mercado de varejo, alguns estados solicitaram que as concessionárias dispusessem de seus ativos de geração como parte da reestruturação. Estas concessionárias atualmente fornecem somente serviços de transmissão e distribuição aos clientes que compram energia elétrica de outras empresas.

A competição levou a mudanças significantes na operação da rede do sistema elétrico, composto de unidades geradoras e linhas de transmissão de alta tensão que constituem o mercado atacadista de energia. Mais energia elétrica está sendo transmitida a partir de maiores distâncias em um sistema de transmissão, que foi inicialmente projetado para fornecer uma quantidade de energia limitada entre concessionárias vizinhas. As concessionárias, que eram as únicas responsáveis por fornecer a geração adequada para a demanda necessária, agora compram uma substancial quantidade de energia do mercado atacadista, confiando que produtores independentes forneçam a geração negociada. Do ponto de vista tecnológico, esta reestruturação tem criado muitos efeitos imprevistos que aumentaram a vulnerabilidade do setor elétrico. Em função deste modelo, as empresas concessionárias estão mais interconectadas do que nunca, o

que não somente fornece mais pontos de entrada para um atacante, mas também aumenta a probabilidade do dano provocado maliciosamente se espalhar por outros sistemas [26]. Este tópico foi alvo de um estudo feito em 1995 pelo "*National Security Telecommuncation Advisory Committee Information Assurance Task Force*". Este estudo incluiu entrevistas e discussões com representantes de toda a indústria de energia elétrica dos Estados Unidos e concluiu com várias recomendações para os segmentos de governo e das companhias de energia elétrica [49]. Exemplos de incidentes com o sistema elétrico norte-americano desde 1965 podem ser encontrados em [30].

Há aproximadamente 5000 unidades de geração de energia elétrica nos Estados Unidos, produzindo cerca de 800.000 MW [25]. A despeito do aumento da oferta de energia por produtores independentes no mercado atacadista, ainda existem inúmeras interrupções de fornecimento de energia em diversas regiões do país, causado por problemas advindos da operação do mercado atacadista e das barreiras para se construir novas usinas. Nos próximos 10 anos espera-se que a demanda de energia elétrica cresça cerca de 30%, e mais de 200.000 MW de nova capacidade sejam necessários. Contudo segundo os planos atuais a capacidade de transmissão crescerá somente 4%, criando sérios problemas de transporte, congestionamento e de confiabilidade.

Os Estados Unidos da América (EUA) não possui um sistema único integrado de transmissão. Ao invés disso, existem 4 sistemas integrados (vide Figura 3.6). Estes sistemas integrados regionais formam uma rede internacional, pois englobam EUA, Canadá e parte do México. As transações entre estes quatro sistemas são limitadas, pois eles são interconetados em poucas localizações, de tal forma que, para propósitos práticos eles podem ser vistos como sistemas isolados. Existem cerca de 377.000 km de

linhas de transmissão na América do Norte, dos quais cerca de 292.000 km estão situados nos EUA[25]. Analistas avaliam em cerca de 800 bilhões de dólares o valor do sistema de transmissão norte-americano. Em 2000 somente o sistema de transmissão e distribuição foram estimados em 358 milhões de dólares [30].

Devido ao seu tamanho, a infra-estrutura de energia elétrica dos EUA possui pontos fortes e pontos fracos (vulnerabilidades) no que diz respeito a ameaças físicas e cibernéticas. Isto faz com que seja impossível garantir a segurança do sistema como um todo. Mas, em função da natureza regionalizada do sistema, estas ameaças ficariam restritas a certa região [26]. Além da possibilidade de erro humano, efeitos econômicos e impactos do mercado de energia, o sistema elétrico atual é vulnerável a desastres naturais e ataques intencionais. Em novembro de 2001, motivados pelos ataques de 11 de setembro, o "*Electric Power Research Institute – EPRI*" (www.epri.com) realizou uma pesquisa em que aponta três ameaças potenciais ao sistema elétrico norte-americano [30]:

- Ataques ao sistema elétrico;
- Ataques pelo sistema elétrico;
- Ataques através do sistema elétrico afetando outras infra-estruturas.

O "*US Department of Energy*" designou o "*North American Electric Reliability Council – NERC*" (http://www.nerc.com/) como o coordenador do setor de energia elétrica para Proteção de Infra-estrutura Crítica. A missão do NERC é melhorar a confiabilidade e segurança do sistema integrado de energia elétrica na América do Norte. Para obtenção deste objetivo o NERC desenvolve e determina padrões de confiabilidade, monitora o sistema integrado, audita proprietários, operadores e usuários

em relação à resposta a ataques e prepara treinamentos para seus clientes. O NERC serve também como centro repositório de informações e análise do setor elétrico ("*Electric Sector Information Sharing and Analysis Center- ESISAC*" - http://www.esisac.com/). Neste site encontramos diversas informações, alertas, avisos e padrões estabelecidos pelo NERC para Proteção de Infra-estrutura Crítica do setor elétrico e compartilhados com seus diversos membros, bem como os níveis de alerta de ameaças para o "*Homeland Security Advisory System*", DOE, Comissão Nuclear e Setor Elétrico. A Figura 3.7 apresenta a "*home page*" deste site. Já o "*Critical Infrastructure Protection Commitee – CIPC*" (http://www.nerc.com/~filez/cip.html), coordena as iniciativas na área de segurança do NERC, com foco em segurança cibernética, física, e operacional. Além disso, o NERC trabalha em conjunto com o "*US Department of Homeland Security*" (http://www.dhs.gov/index.shtm) e o "*Public Safety and Emergency Preparedness Canada*" (http://www.psepc-sppcc.gc.ca/) para garantir que as funções de proteção da infra-estrutura crítica estejam perfeitamente integradas e coordenadas entre os governos dos EUA e Canadá.

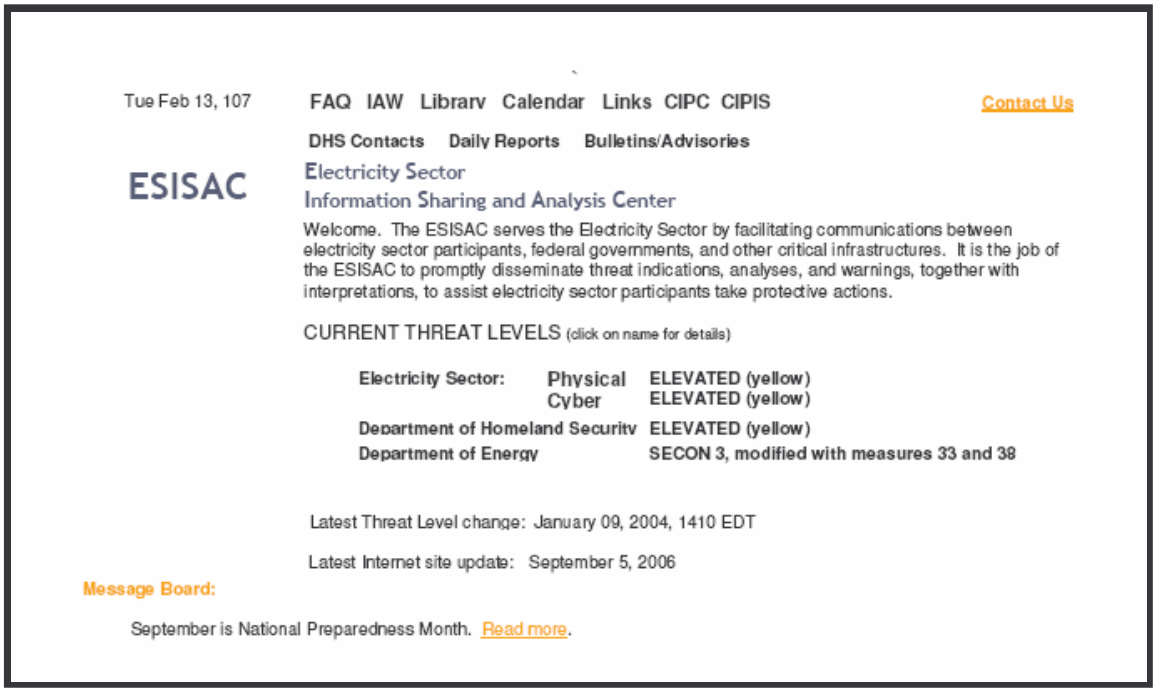


Figura 3.7 - Home page do ESISAC (Fonte: http://www.esisac.com).

O "*The Energy Policy Act 2005*" [27] autorizou a criação de uma Organização Auto-Regulatória de Confiabilidade Elétrica – "*Electric Reliability Organization – ERO*" que se estende por toda América do Norte. A legislação respeita a característica internacional do sistema elétrico global garantindo que o ERO aplica-se e recebe o devido reconhecimento e aprovação das autoridades governamentais do Canadá. Em julho de 2006, o FERC certificou o NERC como o ERO para os EUA. Como ERO, o NERC está sujeito à auditagem pelo FERC e por autoridades governamentais canadenses.

O NERC tem uma importante função na proteção do sistema elétrico servindo como o ponto focal na coordenação da troca de informações na questão de infra-estruturas críticas entre a indústria de energia elétrica e o governo federal. Através do NERC, o governo e a indústria trabalham em conjunto para proteger a infra-estrutura do setor elétrico de ataques físicos e cibernéticos. Esta coordenação garante que a indústria é capaz de falar de forma única e tomar ações de maneira consistente e efetiva. Neste sentido, duas iniciativas do NERC devem ser salientadas:

- "*Security Guidelines*" para o setor elétrico: O NERC criou um compêndio de melhores práticas para proteger instalações críticas contra um amplo espectro de ameaças físicas e cibernéticas. O "*Security Guidelines for Electricity Sector V. 3.0*" [28] inclui tópicos como avaliação de vulnerabilidade e risco, continuidade de negócios, segurança física e cibernética e proteção de informações sensíveis.
- "*Cyber Security Standards*": O NERC adotou em 2006 o "*Cyber Security Standards CIP-002-009*" [29]. Estes padrões estabelecem os requisitos mínimos necessários para garantir a segurança na troca eletrônica das

informações necessárias para suportar a confiabilidade e a operação do sistema elétrico. Eles reconhecem as diferentes funções de cada entidade na operação do Sistema, a criticabilidade e a vulnerabilidade destas instalações e os riscos aos quais eles estão expostos.

Em face da importância que representa a proteção da infra-estrutura do setor elétrico, foi criado o "*PowerSec Initiative*" [30] que é uma aliança formada pelo EPRI, organizações industriais, especialistas da indústria e concessionárias para tratar como as ameaças cibernéticas afetam os equipamentos operacionais e de controle das concessionárias de energia elétrica. Esta iniciativa deverá avaliar o estado de prontidão da indústria atual, identificar as falhas e especificar as melhores práticas existentes para sanar estas falhas. O foco desta iniciativa são os Sistemas SCADA e EMS, ambos os quais são identificados como sistemas críticos para a segurança. É importante salientar que as informações coletadas por esta iniciativa complementam os padrões ora em desenvolvimento/aplicação pelo NERC (CIP-002-009) e pelo FERC.

Numa colaboração público-privada entre o governo e empresas lideres do setor de energia, foi desenvolvido em 2006 o documento chamado "*Roadmap to Secure Control Systems in the Energy Sector*" [51]. Trata-se de um documento que procura delinear estratégias para a segurança dos sistemas de controle dos setores de energia elétrica, petróleo e gás natural num horizonte de 10 anos. Os principais pontos deste documento são:

- Definir uma estratégia de consenso que articule as necessidades de segurança cibernética entre proprietários e operadores do setor de energia;

- Produzir um amplo plano para melhorar a segurança, confiabilidade e funcionalidade dos sistemas de controle de energia para os próximos 10 anos; e
- Guiar os esforços da indústria, academia e governo e ajudar a clarificar como cada grupo de executivos do setor de energia pode contribuir para planejar, desenvolver e disseminar as soluções para segurança.

O documento aborda os seguintes aspectos dos sistemas de controle da indústria de energia:

- Setores de energia elétrica, petróleo, gás e telecomunicações;
- Sistemas legados e de próxima geração;
- Atividades de curto, médio e longo prazo; e
- Pesquisa e desenvolvimento, testes, melhores práticas, treinamento, educação, políticas, padrões e protocolos, compartilhamento de informações e implementação.

Na visão do documento, em 10 anos os sistemas de controle para aplicações críticas serão projetados, instalados, operados e mantidos para resistir a um ataque cibernético intencional sem nenhuma perda de função crítica. Para alcançar esta visão, o documento delineia uma estrutura estratégica formada por 4 objetivos que representam os principais pilares para uma proteção estratégica efetiva:

- Medidas e avaliação de postura de segurança;
- Desenvolver e integrar medidas de proteção;
- Detectar invasão e implementar estratégias de resposta; e
- Manter as melhorias de segurança.

Para obter estes 4 objetivos, o documento relaciona os pontos fundamentais e os respectivos prazos de implementação para os próximos 10 anos. Ele propõe uma estrutura coerente que mapeia quais os esforços e investimentos atualmente em execução nos setores público e privado e ajuda a lançar novos projetos avançados para a segurança de sistemas de controle. O documento faz uma extensa análise dos sistemas de controle para o setor de energia, abordando seus diversos aspectos operacionais, bem como o uso de novas tecnologias de informação, culminando com a definição das estratégias para melhorar a segurança dos sistemas de controle.

3.3 INFRA-ESTRUTURA DE ENERGIA ELÉTRICA DA UNIÃO EUROPÉIA

Na Europa os serviços de transmissão de energia elétrica, bilaterais ou multilaterais, concordam com as regras do setor de energia e as melhores práticas fixadas pelo "*Union for the Co-ordination of Transmission of Electricity – UCTE*" (http://www.ucte.org/). Por mais de 50 anos, UCTE tem operado um dos maiores sistemas síncronos interconectados do mundo, assegurando entrega confiável de energia para mais de 450 milhões de clientes. Uma vez que estes sistemas estão interconectados e, por conseqüência, interdependentes, as operações necessitam ser coordenadas. Desta forma, a missão da UCTE é garantir esta operação coordenada com base em regras previamente acordadas pelo sistema interconectado europeu.

A UCTE coordena a operação e o desenvolvimento da rede de transmissão de eletricidade de Portugal à Polônia e da Holanda até a Romênia e Grécia. Trata-se de uma associação de Operadores de Sistemas de Transmissão ("*Transmission System Operator – TSO*") de 24 países da Europa continental, provendo um mercado confiável

para todos os participantes do "*Internal Electricity Market – IEM*". Sua malha consiste de 200.000 km de linhas de transmissão de 400 e 220 kV, centenas de unidades de geração de energia diretamente conectadas ao sistema, além de centenas de subestações de energia. Vide Fig. 3.8. O consumo anual de energia elétrica estimado em 2.300 TWh. A interconexão síncrona significa que sistemas individuais estão conectados e funcionam em conjunto na mesma freqüência. O TSO é o piloto do sistema: ele é responsável pela operação segura do sistema. Isto significa:

- Monitorar a segurança do sistema de transmissão de eletricidade;
- Monitorar a confiabilidade e estabilidade do sistema;
- Balancear o fornecimento e a demanda a todo instante; e
- Manter e desenvolver a infra-estrutura: redes e facilidades técnicas relacionadas.

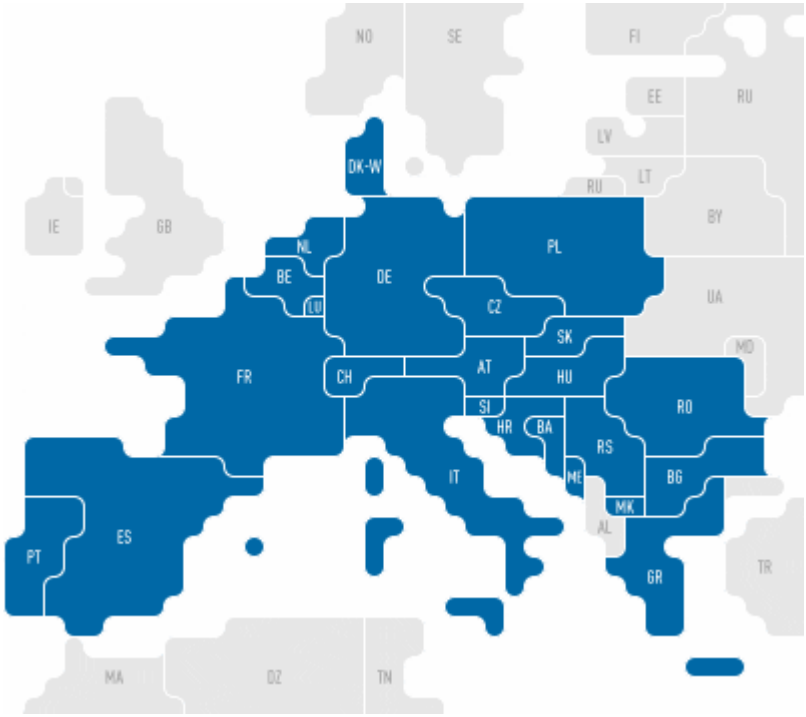


Figura 3.8 - Sistema UCTE (Fonte: http://www.ucte.org/).

No mercado de eletricidade liberalizado que está se desenvolvendo na União Européia, o TSO é o provedor da infra-estrutura e dos serviços de gerenciamento que são pré-requisitos essenciais para o funcionamento do mercado. Como provedor destes serviços para os componentes do mercado (produtores, comercializadores e fornecedores de eletricidade), os TSOs não possuem somente a responsabilidade técnica para a operação do sistema, mas também são responsáveis pelo acesso justo e não discriminatório a estes serviços pelos participantes do mercado.

O aumento excessivo de fluxo através das fronteiras e a reestruturação do setor de eletricidade, separando concessionárias anteriormente integradas verticalmente, em empresas separadas de geração, transmissão e distribuição, resultaram na necessidade de se criar padrões europeus de segurança e confiabilidade obrigatórios para todos TSO interconectados, e num último passo, para todos os clientes do sistema.

O sistema de transmissão do UCTE é dividido em áreas de controle – mais tipicamente países, embora algumas concessionárias estejam juntando-se para formar um bloco de controle único. Entende-se por bloco de controle um subsistema tecnicamente e geograficamente demarcado capaz de operar independentemente em caso de emergências. Como exemplo cita-se o CENTREL, que consiste de várias áreas de controle, como mostrado na Figura 3.9. Compõem o CENTREL os países como Polônia, República Checa, Eslováquia e Hungria, Eslováquia Um centro de controle gerencia a operação do sistema de potência dentro da área de controle (tais como o despacho de geradores sob seu controle) e coordena suas atividades com as concessionárias vizinhas.

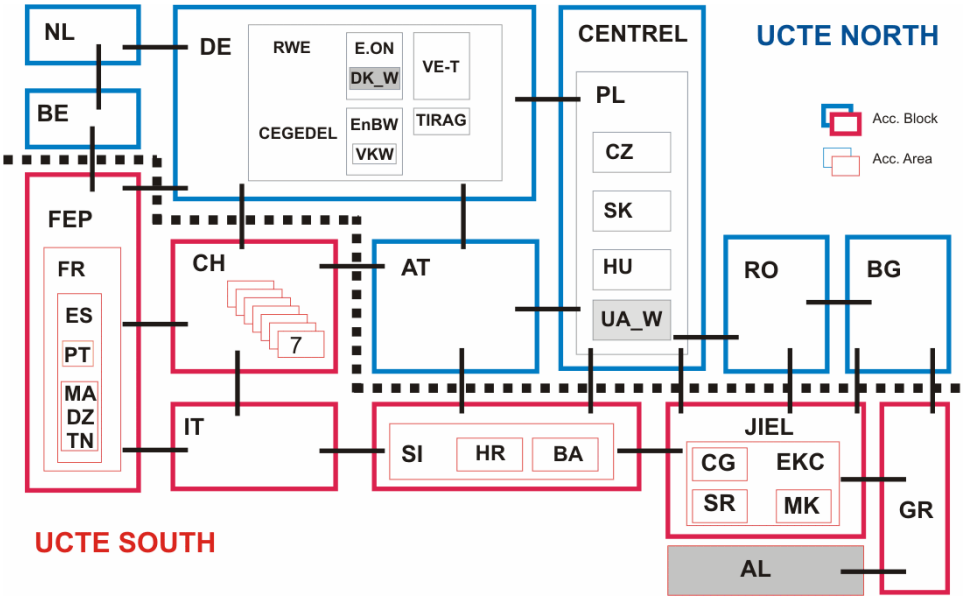


Figura 3.9 – Áreas de Controle da UCTE (Fonte: http://www.ucte.org/).

A operação deste sistema altamente interconectado requer uma operação muita próxima entre os TSOs envolvidos de acordo com regras previamente estabelecidas. O conjunto destas regras forma o "*Operation Handbook*", reunindo em seu conteúdo as regras técnicas e princípios estabelecidos no passado pela UCTE para a operação de redes interconectadas. Para evitar dúvidas em relação à importância do "*Operation Handbook*", cada membro deve assinar um acordo multilateral (MLA), assumindo a sua aquiescência ao referido manual.

3.4 Infra-estrutura de Energia Elétrica do Brasil

O setor elétrico brasileiro tem passado por grandes transformações, migrando de uma configuração centrada no monopólio estatal com um único provedor dos serviços e investidor para um novo modelo de mercado, com a participação de múltiplos agentes e

investimentos compartilhados com o capital privado. Dentre as principais adequações estruturais podemos citar:

- Exploração dos serviços de energia elétrica por terceiros;
- Controle e operação dos sistemas elétricos de forma centralizada;
- Livre acesso e uso das redes elétricas;
- Segmentação das atividades setoriais (geração, transmissão, distribuição e comercialização);
- Criação e regulamentação da comercialização de energia elétrica; e
- Criação do consumidor livre.

As leis 10.847 e 10.848 de 15 de março de 2004 estabeleceram:

- Agência Nacional de Energia Elétrica - ANEEL (www.aneel.org.br): órgão regulador, responsável pela normatização das políticas e diretrizes estabelecidas e a fiscalização dos serviços prestados;
- Operador Nacional do Sistema Elétrico - ONS (www.ons.org.br): órgão responsável pela coordenação e a supervisão da operação centralizada de geração e transmissão do sistema interligado; e
- Câmara de Comercialização de Energia Elétrica – CCEE (www.ccee.org.br).
- A Empresa de Estudos Energéticos – EPE (www.epe.org.br): Vinculada ao Ministério de Minas e Energia, tem por finalidade prestar servicos na área de estudos e pesquisas destinadas a subdisiar o planejamento do setor energético.

Além disso, estas leis estabeleceram, também, o Conselho Nacional de Políticas Energéticas – CNPE e o Comitê de Monitoramento do Setor Elétrico. A Figura 3.10 apresenta as principais instituições do atual modelo setorial elétrico brasileiro.

O sistema elétrico nacional é composto pelo Sistema Interligado Nacional (SIN) e pelos sistemas isolados, localizados principalmente no norte do país. A Figura 3.11 mostra as principais interligações do sistema brasileiro.

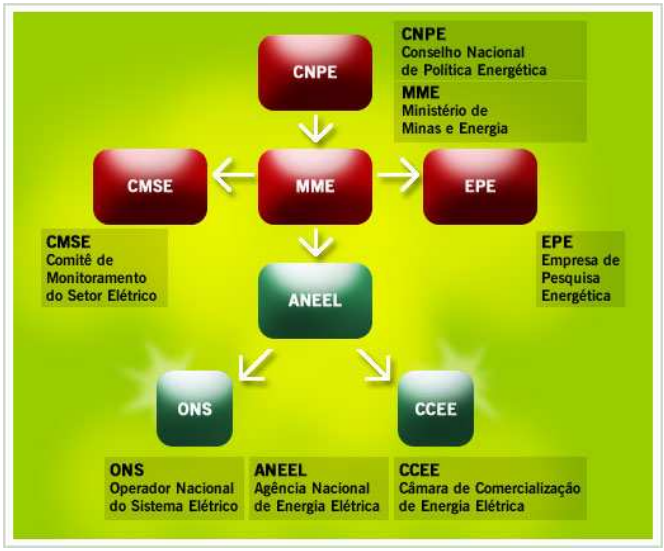


Figura 3.10 - Principais instituições do atual modelo setorial elétrico brasileiro (fonte: http://www.ons.org.br/institucional/relacionamentos.aspx)

O SIN é formado por empresas do sul, sudeste, centro-oeste, nordeste e parte da região norte. Apenas 3,4% da capacidade de produção de eletricidade do país encontram-se fora do SIN. O sistema de produção e transmissão de energia elétrica do Brasil é um sistema hidro-térmico de grande porte, com forte predominância de usinas hidrelétricas e com múltiplos proprietários. Segundo dados do ONS, o SIN é responsável pelo atendimento de cerca de 98 % do mercado brasileiro de energia

elétrica. Ao final de 2005, a capacidade instalada do SIN alcançou a potência de cerca de 84.000 MW, dos quais cerca de 70.000 MW são gerados por usinas hidrelétricas. A rede básica de transmissão (tensões acima de 230 kV) atingiu em dezembro de 2005 cerca de 83.000 km, englobando 851 circuitos de transmissão. O Sistema de Informações Geográficas Cadastrais do SIN – SINDAT (http://www.ons.org.br/conheca_sistema/dados_tecnicos.aspx) disponibiliza informações relevantes do sistema. Segundo o SINDAT, existem 560 usinas e subestações cadastradas e 1079 linhas de transmissão formando a Rede de Operação do ONS.

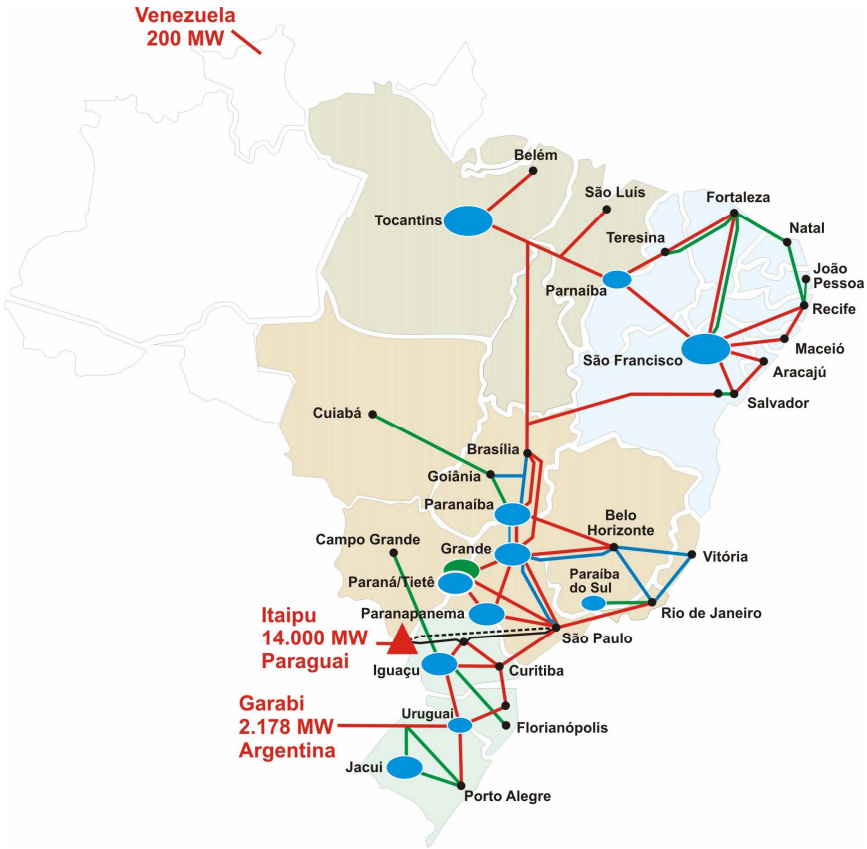


Fig. 3.11 Sistema Elétrico Nacional (fonte: ww.ons.org.br)

A operação integrada do SIN ocorre dentro dos padrões estabelecidos nos Procedimentos de Rede, objetivando atender simultaneamente aos requisitos de segurança elétrica e à minimização dos custos operativos. Os Procedimentos de Rede

são documentos normativos elaborados pelo ONS, com participação dos agentes, e aprovados pela ANEEL, e definem os requisitos necessários à realização das atividades de planejamento da operação eletroenergética, administração da transmissão e operação em tempo real no âmbito do SIN. Atualmente o ONS, atendendo a resolução REN 115/2004 da ANEEL, está realizando a revisão destes Procedimentos.

Durante a realização do SECGOV-2006 (http://www.secgov.com.br), o ONS apresentou "uma série de projetos para segurança elétrica, entre os principais podemos citar o "Plano de Ampliações e Reforços da Rede Básica do SIN", que irá avaliar as condições de segurança para o próximo triênio e propõe obras de ampliações e reforços das instalações existentes, bem como novas obras em sintonia com o planejamento da expansão do SIN" [31]. Outro projeto abordado foi o "Planejamento Elétrico da Operação" com o objetivo de aprofundar e detalhar os estudos de segurança.

Capítulo 4

FUNDAMENTOS DE REDES

Este capítulo apresenta os principais fundamentos teóricos em redes de computadores necessários para o entendimento dos potenciais problemas de segurança advindo do uso de protocolos TCP/IP. São abordados também temas relativos a redes industriais e Sistemas SCADA.

4.1 INTERNET E INTRANETS

4.1.1 Internet

A Internet pode ser considerada como uma "Rede de Redes". Ela é baseada no protocolo padrão para comunicação entre redes chamado TCP/IP ("Transmission Control Protocol & Internet Protocol"). Qualquer rede que usa este conjunto de protocolos pode se integrar à rede mundial Internet. Ela foi concebida para promover o compartilhamento de dados de forma eficiente utilizando diversos tipos de enlaces físicos e de largura de banda. Estes grandes objetivos levaram a uma rede com total ausência de medidas de segurança em seus protocolos. Portanto a Internet é conveniente, eficiente, extremamente efetiva, mas fundamentalmente insegura.

Além das aplicações como correio eletrônico e transferência remota de arquivos, a Internet experimentou um crescente aumento de popularidade com desenvolvimento

dos protocolos, servidores e navegadores de “World Wide Web – WWW”, que possibilitaram o uso comercial da infra-estrutura da rede mundial.

As redes corporativas ou industriais que não utilizam o conjunto de protocolos TCP/IP são consideradas isoladas, separadas da Internet. Trata-se de redes completamente seguras contra ameaças externas, mas de utilidade limitada.

Em resumo, enquanto uma conexão Internet produz claros benefícios, esta mesma conexão deve ser feita com todo cuidado para não trazer também riscos inaceitáveis.

4.1.2 Intranet

Uma “intranet” é uma rede de redes “intramuros”. Mais e mais as empresas estão descobrindo que a tecnologia Internet pode ser usada para interconectar suas redes internas, provendo a comunicação e o compartilhamento de recursos e informações de forma controlada.

As intranets utilizam os mesmos protocolos e a tecnologia da Internet para permitir que usuários de uma rede interna se comuniquem com a outra rede interna, fornecendo diversos tipos de serviços inerentes a natureza da empresa. Em intranets corporativas é comum o controle de acesso a informações sensíveis entre as redes internas que compõem a intranet. Portanto é necessário aplicar os mesmos cuidados que se aplicam a troca de informações com redes externas.

4.1.3 Arquitetura TCP/IP

TCP/IP é uma família modular de protocolos, fornecendo uma ampla gama de funções e aplicações. Em geral utilizamos o modelo de referência OSI, para compararmos os diferentes protocolos presentes no conjunto de protocolos TCP/IP, desde o nível físico até às funções de aplicação.

4.1.4 Modelo de Referência OSI

Trata-se de um modelo conceitual baseado em camadas, as quais servem para identificar as diversas funções fornecidas pela rede. O Modelo de Referência OSI se baseia em 7 camadas, cada uma delas fornecendo uma função específica e interdependente entre as camadas adjacentes. Este modelo facilita a discussão dos vários serviços fornecidos por uma rede.

As sete camadas do modelo OSI são enumeradas a seguir:

- **Camada Física**: Diz respeito ao meio físico utilizado para conectar diferentes sistemas numa rede.
- **Camada de Enlace de Dados**: Define como a informação é transmitida através da camada física. Esta camada também trata os erros, a retransmissão da informação e o relatório de falhas para a próxima camada.
- **Camada de Rede**: É utilizada para definir o modelo de endereçamento dos sistemas na rede, ou seja, sua identificação. Também é responsável pela transmissão dos dados entre os sistemas, empacotando-os de tal forma que a camada de enlace de dados possa entregá-los à camada física.

- **Camada de Transporte**: Esta camada fornece os serviços confiáveis para a camada de rede, verificando se ela esta operando eficientemente. Caso contrário requisita a retransmissão ou retorna um erro para a camada acima.
- **Camada de Sessão**: Esta camada é responsável por estabelecer e destruir as conexões entre os sistemas, as aplicações ou os usuários. Ela recebe a requisição da camada superior e negocia a conexão usando as camadas inferiores.
- **Camada de Apresentação**: Fornece um conjunto consistente de interfaces para uso das aplicações e serviços quando estabelecendo a conexão, através da camada de sessão.
- **Camada de Aplicação**: Esta camada fornece a interface de rede aos protocolos da aplicação do usuário.

4.2 REDES DE COMPUTADORES COM PROTOCOLO TCP/IP

4.2.1 Comparando TCP/IP com o Modelo de Referência OSI

O conjunto de protocolos TCP/IP não se encaixa perfeitamente ao Modelo de Referência OSI. A Figura 4.1 mostra a comparação do conjunto de protocolos TCP/IP e o Modelo de Referência OSI. Nota-se que o conjunto TCP/IP não fornece os serviços da camada física e da camada de enlace de dados diretamente. Ele deixa para que o Sistema Operacional forneça tais serviços, em função da topologia de rede adotada. Desta forma, alguns protocolos e serviços mapeiam-se diretamente, enquanto outros não possuem um protocolo ou serviço correspondente. Este arranjo é chamado de pilha TCP/IP ou "*TCP/IP Suíte*".

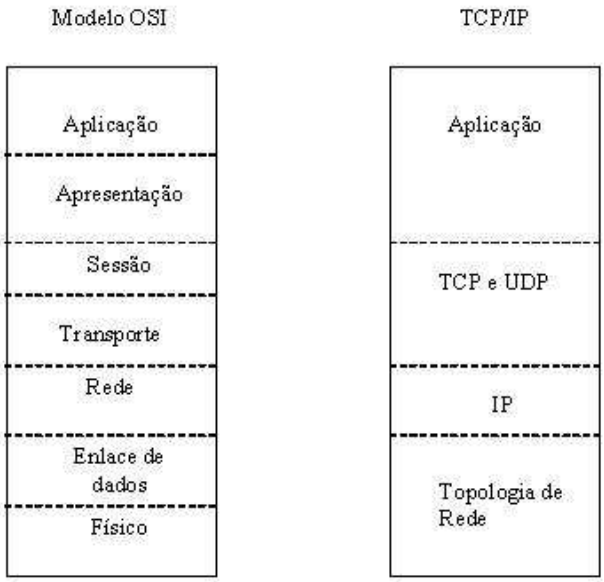


Figura 4.1 - Comparação do Modelo OSI e TCP/IP

As camadas do conjunto de protocolos TCP/IP e seus respectivos serviços são:

- **Camada de Aplicação:** Suporta a implementação da aplicação fornecendo serviços tais como navegadores (HTTP), serviços de nomes de domínio (DNS – "*Domain Naming Service*"), correio eletrônico (SMTP- "*Single Mail Transfer Protocol*"), transferência de arquivos (FTP – "*File Transfer Protocol*"), dentre outros.
- **Camada de Transporte:** A Camada de Transporte possui dois protocolos: TCP (Transport Control Protocol), que é referenciado como um protocolo confiável, pois possui mecanismos que garante a monitoração e a entrega dos dados, e o UDP ("*User Datagram Protocol*"), que realiza um transporte mais simples sem correção de erro e serviços de controle de fluxo ("*Best effort*").
- **Camada de Rede:** Representado pelo principal protocolo, o "*Internet Protocol*" (IP), ele é o responsável por seguir os endereços dos dispositivos na rede,

determinado como os datagramas IP são entregues. Desta forma ele age como uma representação virtual da rede.

- **Camada de Enlace da Dados:** Os protocolos deste nível estão envolvidos com o "*Network Interface Controller – NIC*", que fazem a interface entre as camadas de rede e enlace de dados, sendo os responsáveis pelo endereçamento no nível físico.

4.2.2 Protocolos e serviços do Conjunto TCP/IP

Observando a Figura 4.2, podemos notar que sempre que os dados são trocados entre 2 aplicações através de uma rede TCP/IP, cada camada provê um determinado tipo de serviço.

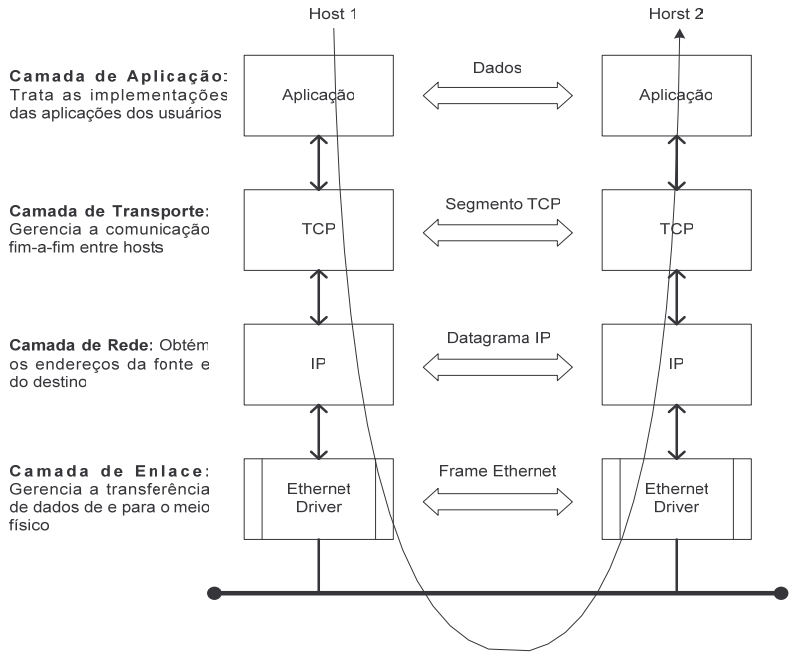


Figura 4.2 - Modelo de comunicação TCP/IP.

À medida que os dados passam através de cada uma das camadas, os pacotes são gerados contendo 2 elementos distintos: *Cabeçalho e Dados*, também chamado de

"*payload*". À medida que os dados passam por entre 2 camadas vizinhas ("*peers*"), eles sofrem um processo de *encapsulamento*, onde os dados oriundos da camada anterior (cabeçalho e dados) são empacotados pela camada sucessora juntos com um novo cabeçalho, contendo informações específicas daquela camada, como mostrado na Figura 4.3.

Um ponto importante a salientar neste arranjo é que a atividade de fluxo dos dados, que atravessa toda a pilha TCP/IP do host fonte para o host destino, se realiza através da "conversa" entre a respectiva camada do lado fonte e do lado destino, usando as informações colocadas pelo host no cabeçalho do pacote. Tomando a Figura 4.3 como nossa referência, podemos entender as setas horizontais do processo mostrado na Figura 4.2. Cada camada do lado do host fonte coloca uma informação no seu cabeçalho e o host destino reverte o processo retirando esta informação, camada a camada, para orientar suas ações.

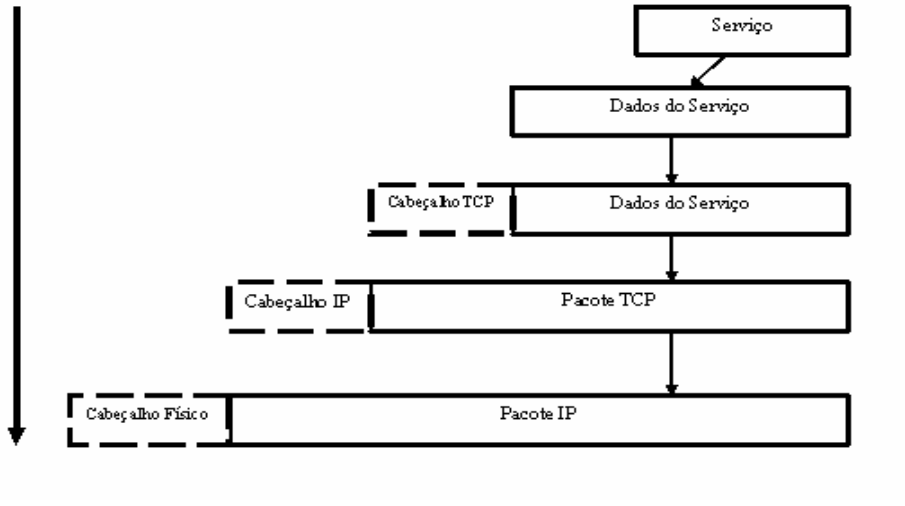


Figura 4.3 - Processo de encapsulamento da informação através das camadas

A Tabela 4.1 apresenta como o protocolo TCP/IP é subdividido em camadas com os respectivos serviços de rede associados.

Tabela 4.1 - Camadas e serviços de redes associados do suíte TCP/IP.

Camada	Serviço de Rede
Aplicação	DNS, telnet, FTP, TFTP, SMTP, HTTP, etc.
Transporte	TCP , UDP
Rede	IP, ICMP
Enlace de Dados	ARP, RARP e interface de rede
Físico	Meio físico

Conforme [32], podemos resumir estes relacionamentos como mostrado na Figura 4.4.

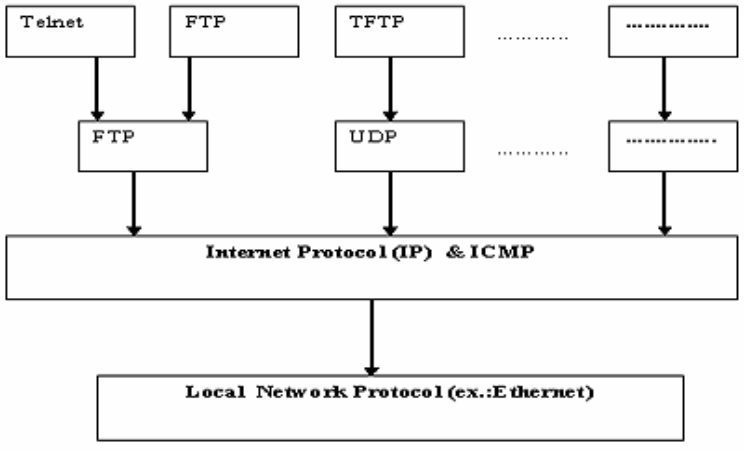


Figura 4.4 - Relacionamentos entre os protocolos.

A Figura 4.5 apresenta a estrutura lógica das camadas de protocolos. Segundo [33], todo computador conectado a uma rede com tecnologia internet possui tal estrutura. Esta estrutura lógica determina o comportamento dentro da rede. As caixas representam o processamento dos dados quando ele passa através do computador e as linhas conectando as caixas mostram o fluxo dos dados. A linha horizontal representa o meio físico, por exemplo, um cabo ethernet. Esta estrutura ajuda a melhor compreensão da interrelaçao dos diversos protocolos e o acesso ao meio físico. Nesta estrutura

observa-se que o módulo TCP, o módulo UDP e o NIC são multiplexadores *n-para-1*. Como multiplexadores eles chaveiam muitas entradas para uma única saída. No sentido inverso do fluxo de dados, eles são demultiplexadores *1-para-n*, pois eles podem chavear 1 entrada para várias saídas de acordo com informações contidas no cabeçalho do pacote.

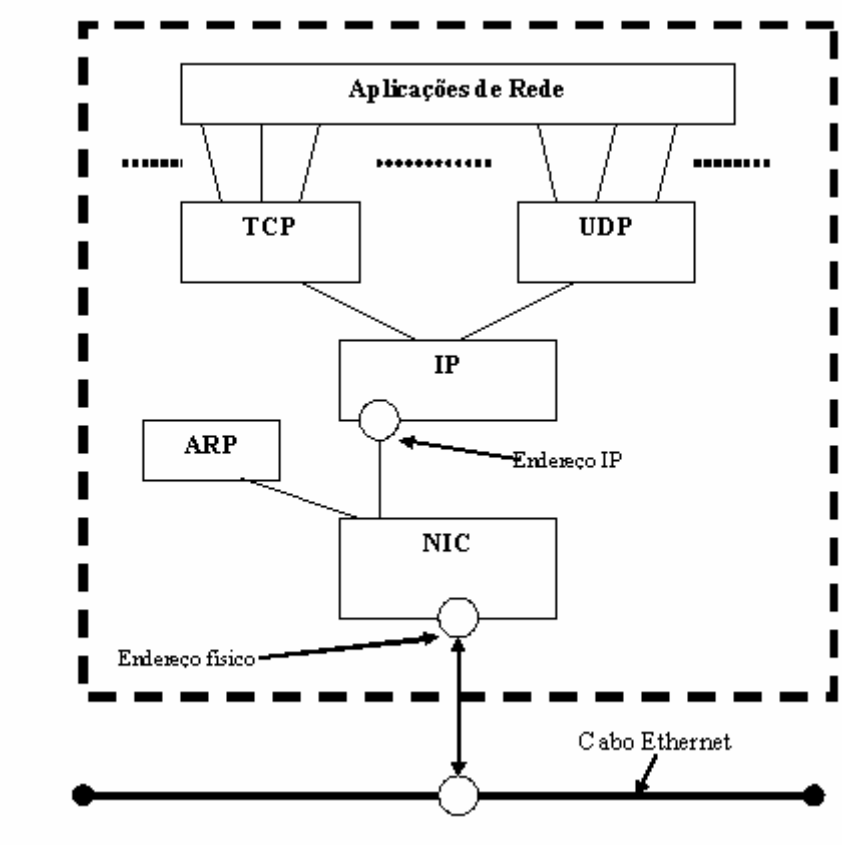


Figura 4.5 - Estrutura lógica de um nó de uma rede.

4.2.3 Serviços de Enlace de Dados

Como representado na Figura 4.5, quando dois dispositivos numa rede comunicam-se entre si, eles não usam somente o protocolo IP. Ao invés disso, eles usam protocolos específicos para o meio escolhido. No exemplo apresentado, os dispositivos num segmento Ethernet usam uma série de impulsos elétricos pré-definidos

para se comunicarem entre si e definidos pelo protocolo Ethernet. Outros exemplos de protocolos físicos são Token Ring, Frame Relay, FDDI, IEEE802.11, entre outros.

Uma das tarefas do protocolo IP é prover o mecanismo de endereçamento na rede. Da mesma forma os protocolos de acesso ao meio físico devem prover mecanismos para encapsular e disseminar os dados pela rede, bem como os mecanismos para se localizarem. Por exemplo, em redes Ethernet, para cada NIC é definido um endereço físico, chamado "*Media Access Controller Address*", ou simplesmente "*MAC address*". Este endereço único de 48 bits de comprimento é atribuído ao NIC pelo fabricante. Através do processo de resolução de endereço implementado pelo serviço "*Address Resolution Protocol – ARP*", o endereço físico, ou "*MAC address*", é relacionado ao endereço lógico de rede fornecido pelo protocolo IP.

O protocolo ARP trabalha enviando uma mensagem de "*broadcast*" no segmento de rede em que o computador fonte está conectado, requisitando que o dispositivo usando um determinado endereço IP responda, enviando o seu endereço físico. Uma vez o dispositivo destino tenha respondido a requisição, o dispositivo fonte, agora de posse do endereço físico do destino, montará o quadro incluindo o endereço físico do destino e estabelecerá a comunicação, enviando os dados para o mesmo. A mensagem de "*broadcast*" é uma mensagem especial enviada a todos dispositivos conectados a um determinado segmento de rede. As requisições e respostas do protocolo ARP trabalham no nível físico e estão incorporadas diretamente nos quadros produzidos pelos protocolos de baixo nível em uso pelo meio físico.

4.2.4 Protocolo IP

O Protocolo IP fornece o serviço de formatação do datagrama e o mecanismo de endereçamento, que é independente de quaisquer das características das redes individuais que compõem uma rede com tecnologia internet. Em outras palavras, o protocolo IP fornece uma representação virtual para os dispositivos conectados a uma rede. Para que os dados sejam enviados para um endereço IP, eles devem ser encapsulados e transmitidos de acordo com as regras de cada uma das redes intermediárias. O datagrama IP fornece as informações necessárias para os dispositivos fonte, intermediário e destino. Portanto cabe ao protocolo IP o roteamento das mensagens e aos protocolos da camada de enlace de dados a entrega efetiva da mensagem. A Figura 4.6 fornece uma visão de como isto ocorre usando uma conexão via rede discada.

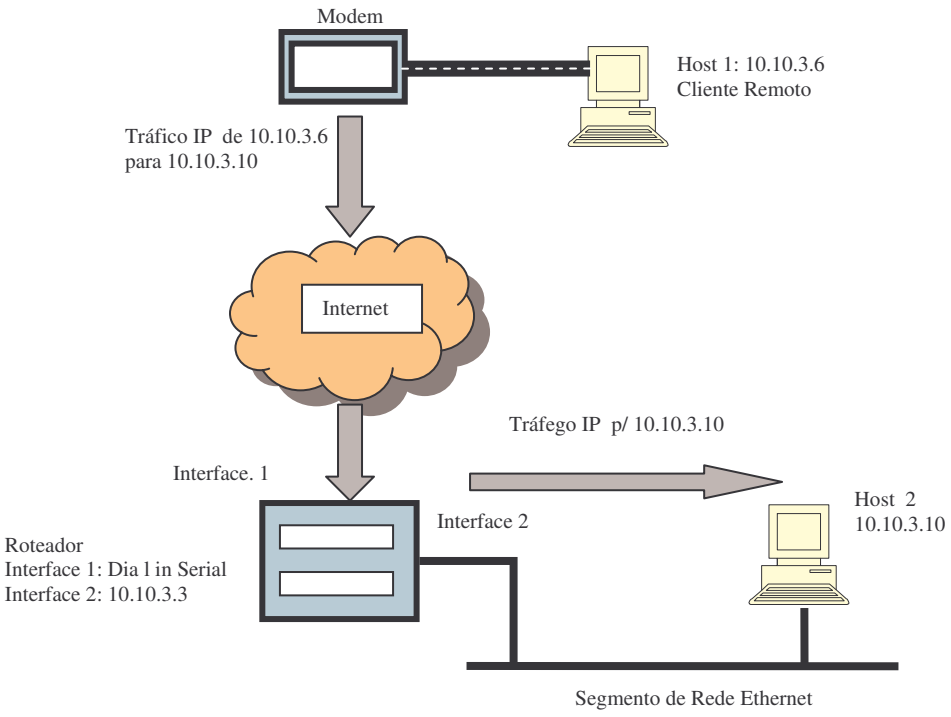


Figura 4.6 - Tráfego IP usando conexão discada sobre rede Ethernet.

O endereço IP é um número de 32 bits dividido em 4 campos de 8 bits. Segundo classificação pré-estabelecida, estes campos são combinados formando 5 classes de endereços, dos quais 3 formam as classes A, B e C, chamadas de endereços "*unicast*", ou seja, 1 para 1. A classe D é chamada de endereço "*multicast*", ou seja, 1 para vários. E a classe E é uma classe reservada. Com relação às classes A, B e C, os endereços são divididos em 2 partes: endereço de rede e endereço do host. Cada classe tem uma combinação diferente destes campos, conforme Tabela 4.2. Esta tabela apresenta as faixas de endereço IP alocadas para cada classe. O padrão aqui descrito chama-se IP Versão 4. Atualmente está-se fazendo a transição para a nova versão, chamada IP Versão 6.

Tabela 4.2 - Espaço de Endereçamento IPV4.

Classe	Rede (Número de Bits)	Host (Número de Bits)	Número de Hosts	Endereço IP inicial	Endereço Ip final
A	8	24	+16 Milhões	0.0.0.0	127.255.255.255
B	16	16	+65.000	128.0.0.0	191.255.255.255
C	24	8	255	192.0.0.0	223.255.255.255

A Figura 4.7 mostra como o cabeçalho de um datagrama IP está organizado. Cada linha do cabeçalho IP tem 32 bits. Cada campo possui um tamanho específico ligado a sua função. Por exemplo, o campo protocolo informa qual o protocolo será usado após o cabeçalho IP (UDP ou TCP). Já o campo TTL ("time to live") especifica o número de "saltos" que restam antes que o datagrama seja considerado "sem possibilidade de entregar" ("*undeliverable*") e seja, então, destruído.

<table>
<tr><td colspan="4">Número de Bits

0.....31</td></tr>
<tr><td>VER</td><td></td><td>TOS</td><td>Comprimento em Bytes</td></tr>
<tr><td colspan="3">Campo identificador</td><td>Frag Offset</td></tr>
<tr><td>TTL</td><td colspan="2">Protocolo</td><td>Checksum do cabeçalho</td></tr>
<tr><td colspan="4">Endereço IP Fonte</td></tr>
<tr><td colspan="4">Endereço IP Destino</td></tr>
</table>

Figura 4.7 - Layout do cabeçalho de um Datagrama IP com 20 bytes.

Outro protocolo presente na camada de rede é o ICMP, "*Internet Control Message Protocol*". De tempos em tempos datagramas IP não conseguem atingir seus destinos. O protocolo IP utiliza, então, outro protocolo, o ICMP, para serviços de relatório de erros. Quando um sistema necessita relatar um problema que impede a entrega do pacote, ele gera uma mensagem ICMP que descreve o problema de forma geral, informando ao dispositivo fonte para que ele possa, então, parar de tentar enviar aqueles datagramas.

Mesmo se dois sistemas são capazes de se comunicar sem problemas, não há garantias de que tudo funcionará bem, pois os dados dentro do datagrama podem estar corrompidos ou pacotes podem se perder sem gerar qualquer mensagem ICMP. O protocolo IP é um protocolo não confiável por definição, e como tal não fornece quaisquer garantias. O ICMP não altera este fato [33].

Existe uma variedade de tipos de mensagens ICMP, embora nem todas sejam para relatar erros. Os exemplos mais conhecidos são o "*ICMP echo*" e o "*ICMP reply*", utilizadas para implementar o comando *"ping"*.

4.2.5 Protocolo de Transporte

Os Protocolos de Aplicação não se comunicam diretamente com o protocolo IP. Eles conversam com 2 protocolos de transporte: TCP ou UDP. A principal função destes protocolos é esconder a rede das aplicações, de tal forma que as aplicações não tenham que tratar com problemas mais básicos de empacotamento, roteamento, etc.

Que protocolo de transporte uma aplicação utiliza é definido pelo tipo de serviço de rede e de gerenciamento necessários à aplicação. TCP é um protocolo confiável, orientado à conexão, fornecendo serviços de correção de erro e controle de fluxo. Quando uma aplicação utiliza TCP, é estabelecido, em primeiro lugar, um circuito virtual de comunicação entre os dois dispositivos que estão se comunicando, garantindo assim a comunicação fim-a-fim. Por sua vez, UDP é um protocolo não confiável, não orientado à conexão e que oferece pouca funcionalidade ao protocolo IP. UDP não mantém uma comunicação fim-a-fim com o dispositivo remoto. Existem muitas aplicações que utilizam um ou outro protocolo de transporte, mas existem também várias aplicações que utilizam ambos.

Tanto UDP quanto TCP utilizam um número chamado de *porta* para estabelecer o caminho de comunicação entre a aplicação e o protocolo de transporte. Trata-se de um número de 16 bits, presente no cabeçalho de mensagem TCP ou UDP. Isto permite o serviço de multiplexagem oferecido por ambos os protocolos, isto é, várias aplicações

podem ser executadas no mesmo dispositivo, usando diferentes números de portas para identificação junto aos protocolos de transporte. Por exemplo, uma aplicação que está oferecendo um serviço espera pacientemente que mensagens cheguem à porta especificada para aquele serviço, conforme mostrado na Figura 4.8. A Tabela 4.3 apresenta números de portas para alguns serviços de rede comuns.

Tabela 4.3 - Aplicações e o número de portas atribuídas.

Aplicação	**Número de Porta/ Protocolo de Transporte**
ftp	21/tcp
telnet	23/tcp
Smtp	25/tcp
DNS	53/udp
DNS	53/tcp

Vale ressaltar que um serviço pode utilizar qualquer número de porta. Contudo, para obter a interoperabilidade, é melhor seguir os valores padrões estabelecidos, como aqueles encontrados no arquivo */etc/services* existentes nos sistemas operacionais baseados em UNIX, conforme mostrado na Tabela 4.3.

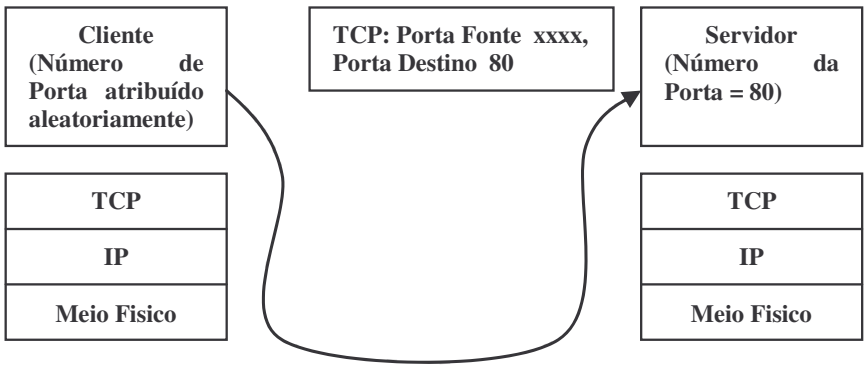


Figura 4.8 - Multiplexagem ao nível de aplicação usando portas.

O termo "*socket*" identifica o par: número da porta e o endereço IP concatendado. O termo "*socket pair*" consiste do "*socket*" dos pontos terminais do circuito virtual estabelecido. Múltiplas conexões entre dois sistemas devem possuir "*socket pairs*" únicos, com ao menos um dos dois terminais tendo um número de porta diferente, conforme mostrado na Figura 4.9.

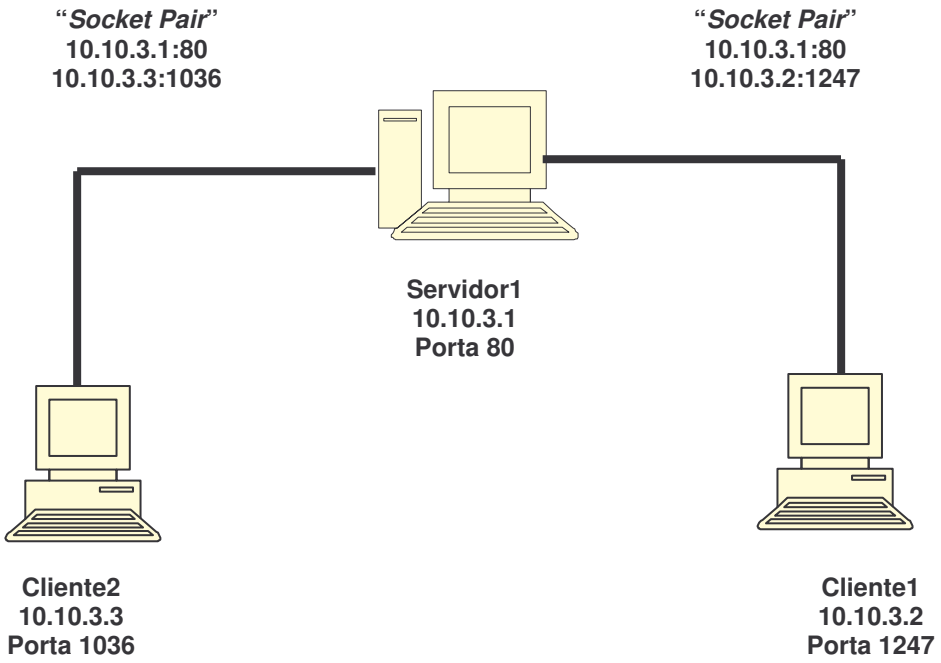


Figura 4.9 - Servidor com 2 conexões usando 2 pares de "*sockets*" distintos.

Embora o conceito de circuito virtual e de número de porta seja distinto, eles estão fortemente interligados. O circuito virtual fornece o transporte gerenciado entre a fonte e o destino, enquanto os números de porta fornecem endereços para que as aplicações os utilizem quando comunicando-se com o servidor. Desta forma é possível ao servidor de aplicação suportar múltiplas conexões de vários clientes através de um endereço de porta único, conforme mostrado na Figura 4.9.

As Tabelas 4.4 e 4.5 apresentam a organização do cabeçalho dos protocolos TCP e UDP. Pelo número de informações presentes no cabeçalho TCP, podemos concluir que se trata de um protocolo bem mais complexo e, portanto, consome mais recursos que o protocolo UDP, tanto do dispositivo fonte quanto do dispositivo destino.

Tabela 4.4 - Campos de uma mensagem UDP.

Campo	Número de Bits	Função
Porta Fonte	2	Identifica o número da porta utilizada pela aplicação que está enviando os dados
Porta Destino	2	Identifica o número da porta utilizada pela aplicação que está recebendo os dados
Comprimento	2	Especifica ao tamanho total da mensagem UDP
Checksum	2	Checksum de toda a mensagem
Dados	vários	Dados da mensagem

Tabela 4.5 - Campos de um segmento TCP.

Campo	Número de Bits	Função
Porta fonte	16	Identifica o número da porta utilizada pela aplicação que está enviando os dados
Porta destino	16	Identifica o número da porta utilizada pela aplicação que está recebendo os dados
Identificador de seqüência	32	A cada byte de dados enviado através do circuito virtual é atribuído um número único. O Identificador de seqüência identifica o número associado com o primeiro byte de dados neste segmento
Identificador de reconhecimento (ack)	32	Identifica o próximo byte de dados que o recipiente espera receber
Comprimento do cabeçalho	4	Especifica o tamanho do cabeçalho TCP
Reservado	6	Reservado
Flags	6	Usado para funções de comutação do circuito virtual
Window	16	Identifica o tamanho do buffer do recipiente em uso no sistema que gerou este segmento
Checksum	16	Checksum de todo o segmento TCP
Urgent Pointer	16	Identifica ao último byte de um dado urgente que deve ser tratado imediatamente
Opções (Se existir)	Vários	
Dados (Se existir)	Vários	Dados presentes no segmento TCP

Através do uso de números de seqüência e dos flags de reconhecimento (ACK), o TCP consegue manter o status da conexão a todo instante, pois cada byte de dados enviado sobre o TCP deve receber um sinal de reconhecimento (ACK). Caso um dos sistemas não receba este sinal, o TCP re-enviará a mensagem em questão. A Figura 4.10 mostra este esquema.

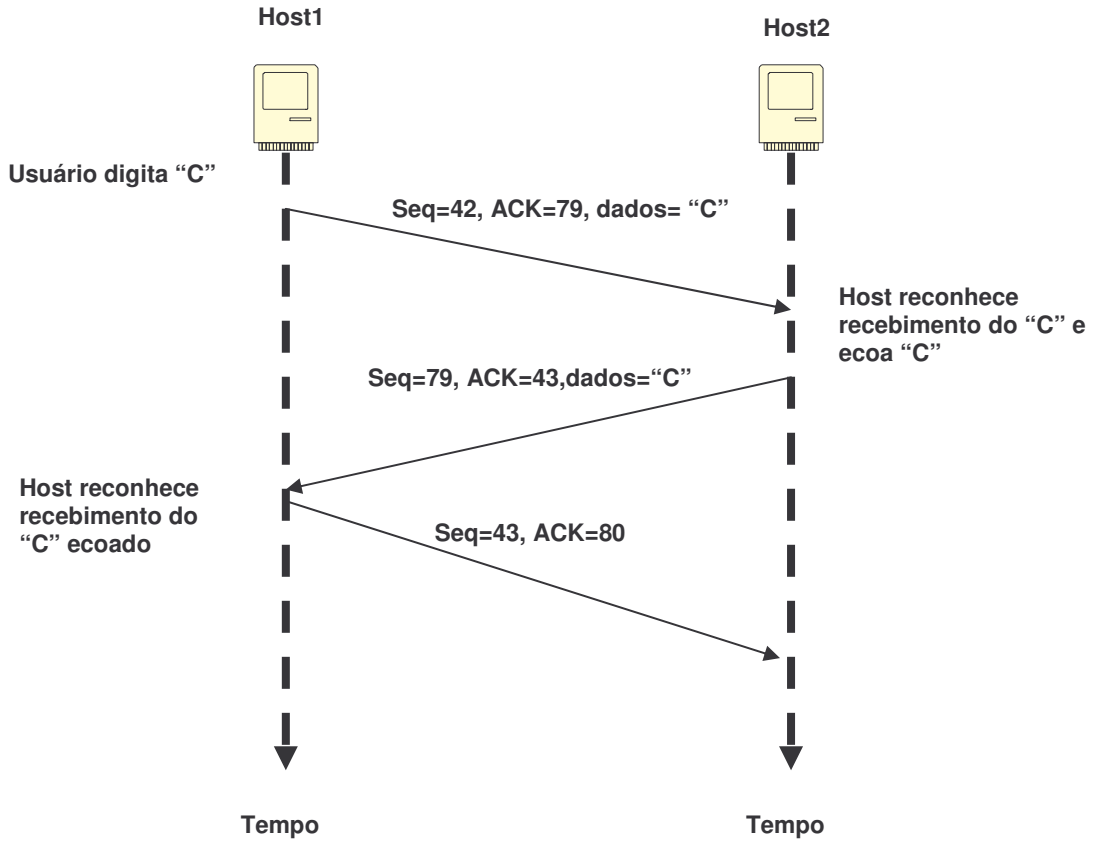


Figura 4.10 - Uso de Número de Seqüência numa transação TCP.

O uso dos números de seqüência permite ao TCP implementar o controle de fluxo e outros serviços no topo do protocolo IP, sincronizando, desta forma, a transferência de dados entre dois dispositivos, conforme mostra a Figura 4.10.

O uso dos números de seqüência permite ao TCP implementar o controle de fluxo e outros serviços no topo do protocolo IP, sincronizando, desta forma, a transferência de dados entre dois dispositivos, conforme mostra a Figura 4.10.

4.2.6 Protocolos de Aplicação

Existe uma variedade de protocolos de aplicação, cada um fornecendo mecanismos padronizados para troca de informações. São exemplos destas aplicações:

- Transferência de arquivos: FTP, Gopher e HTTP;
- Serviços de Correio eletrônico: SMTP, POP3, IMAP4 e NNTP;
- Localizar recursos de rede: DNS, Finger e LDAP; e
- Gerenciamento de Redes: SNMP.

As aplicações do lado do cliente consistem, em geral, de dois componentes distintos:

- O Protocolo de Aplicação, por exemplo, HTTP; e
- A interface para visualização das informações.

Por exemplo, o navegador de web utiliza o protocolo HTTP para recuperar informações, como páginas HTML, de um servidor de web, mas o código para visualização dos dados é um serviço à parte, e não é coberto pelas especificações do protocolo.

Quase todas as aplicações seguem o mesmo modelo básico cliente/servidor: um cliente envia uma requisição de serviço para um servidor. Este, em função da requisição, faz algum tipo de processamento e, possivelmente, retorna algum tipo de

informação ao cliente. As aplicações baseadas em servidor são carregadas pelo sistema operacional e ficam, a seguir, a espera de requisições de conexão. Por sua vez, os clientes somente estabelecem conexões quando alguma ação é requisitada. Toda vez que um protocolo de aplicação abre uma conexão de E/S com um dos protocolos de transporte, ele aloca um número de porta. Desta forma, qualquer tráfego destinado àquela aplicação será roteada para a porta apropriada, conforme mostra a Figura 4.11. Essas aplicações podem abrir muitas conexões simultaneamente, sendo que cada conexão obtém um número de porta. Do lado do cliente cada uma destas conexões, criadas independentemente, terá números de portas únicos. Quanto aos servidores, eles não se importarão se um cliente requer múltiplas conexões, desde que para cada conexão o cliente atribua um número de porta único.

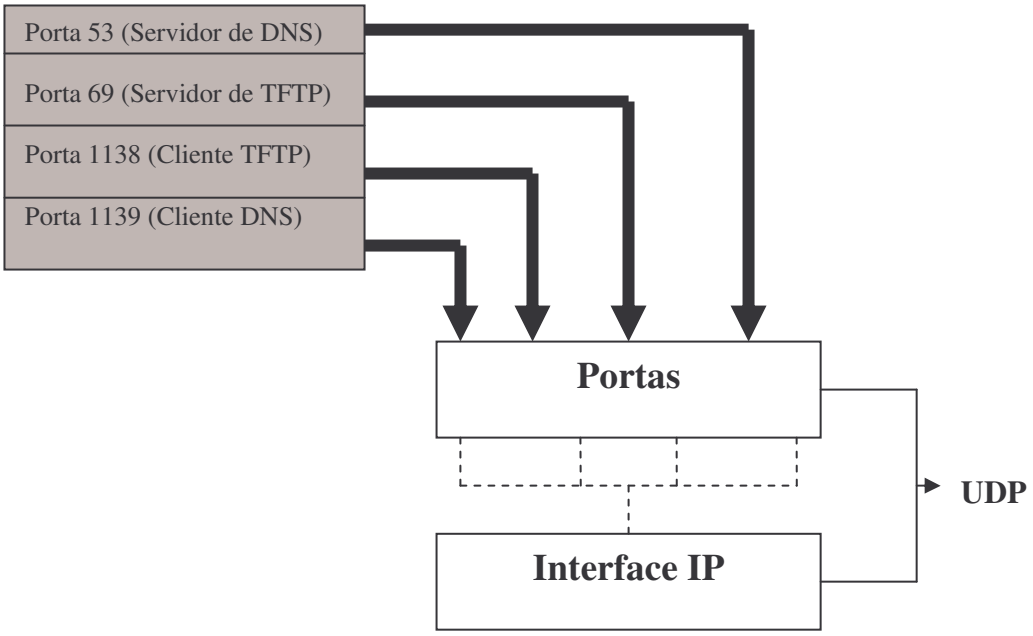


Figura 4.11 - Multiplexagem ao nível da aplicação com número de portas.

4.3 REDES INDUSTRIAIS

Devido aos benefícios oferecidos pelas redes de comunicação de dados, muitas empresas e indústrias têm demonstrado interesse em aplicar esta tecnologia com o propósito de controle industrial e automação em fábrica. Em [34] e [35], encontramos ótimas revisões desta tecnologia em controle industrial. Podemos encontrar exemplos da utilização destas tecnologias em indústrias como manufaturas, geração e distribuição de energia elétrica, fornecimento de água e gás, transporte, petróleo e indústrias químicas, dentre outras. Dependendo do tipo e propósito do sistema de automação, seus componentes podem ser locais, espalhados em uma área geográfica ou mesmo em escala mundial [34].

Existem dois tipos de configurações para este tipo de rede: direto e hierárquico [35]. Tipicamente, redes comunicação para automação industrial são construídas utilizando-se o modelo hierárquico [34], com os níveis variando dos sensores e atuadores na parte inferior da hierarquia a redes locais (LAN – "*Local Área Network*") e, possivelmente, redes WAN ("*Wide Área Network*") no topo. O uso de níveis hierárquicos é necessário devido à necessidade de tratar grande quantidade de dados, nem sempre relevantes a todos os níveis.

A estrutura de um típico sistema de controle distribuído é apresentada na Figura 4.12. No topo da estrutura tem-se a rede corporativa que executa as aplicações de gerenciamento da manufatura e de processos. Na parte intermediária da estrutura tem-se a rede de controle que liga estações de trabalho (Interface Homem-Máquina - IHM), utilizadas pelos sistemas supervisórios, aos controladores de processo. Esta rede de

controle pode ser dividida em diferentes segmentos. Os controladores de processo são por sua vez conectados ao nível inferior da estrutura, chamado de nível de campo ou processo. Neste ponto tem-se os barramentos de campo conectando os dispositivos de campo, tais como sensores e atuadores. Do nível inferior ao topo da estrutura, o tráfego de dados é filtrado e agregado aos servidores especializados situados entre os níveis.

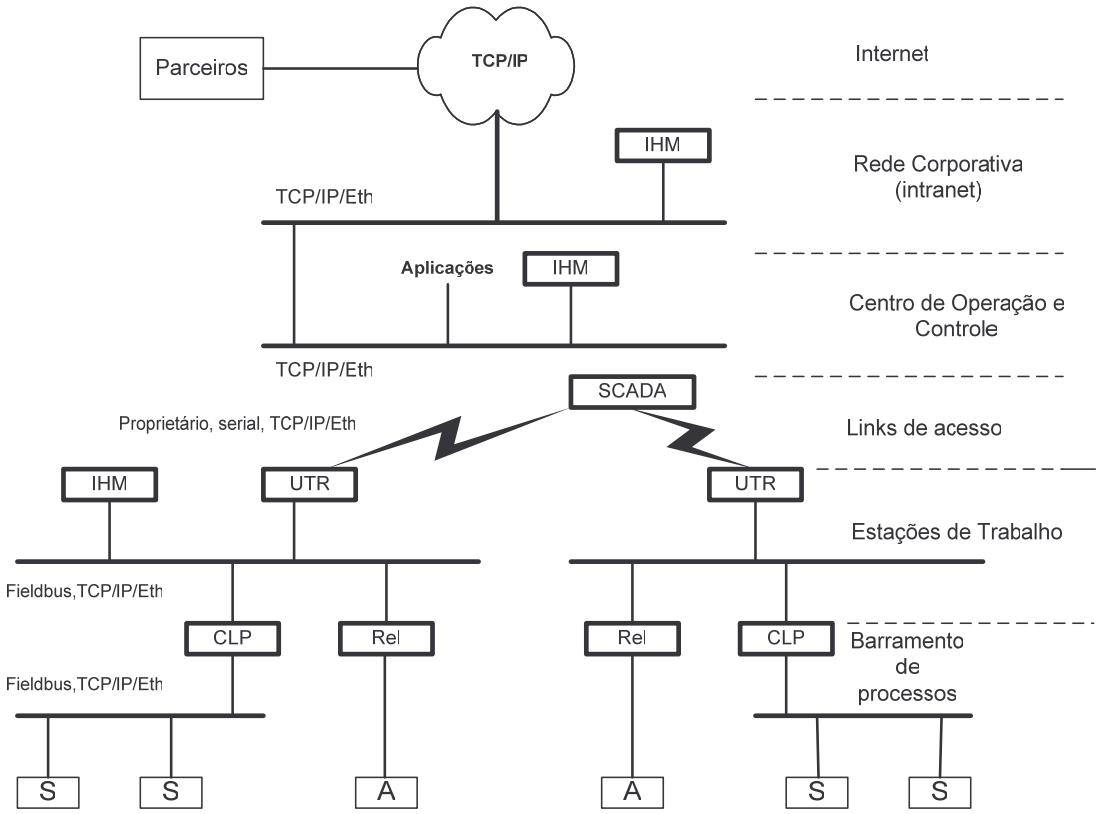


Figura 4.12 - Estrutura Hierárquica de uma Rede Industrial.

Existem vários protocolos de comunicação em uso nos diferentes níveis hierárquicos. As redes dos níveis superiores da hierarquia utilizam na maioria dos casos o conjunto de protocolos TCP/IP. Nas conexões de missão crítica existe a predominância dos barramentos de campo ou conexões dedicadas, embora a tecnologia Ethernet também esteja presente. Barramentos de campo possuem protocolos

específicos, necessitando, portanto, de "*gateways*" para realizar a conversão de protocolo e fornecer uma interface comum para os níveis superiores. Exemplos destas interfaces padrão da indústria são o "*Manufacturing Message Specification – MMS*" (ISO 9506) [36] e os padrões definidos pelo "*Open Process Control Foundation – OPC*" [37].

Uma das funções destas interfaces padrões é esconder os detalhes dos protocolos de barramento de campo, permitindo projetar e implementar eficientemente as aplicações de automação. Muitas das implementações de MMS e OPC estão construídas sobre o conjunto de protocolos TCP/IP. Veja o exemplo da interface MMS na figura 4.14.

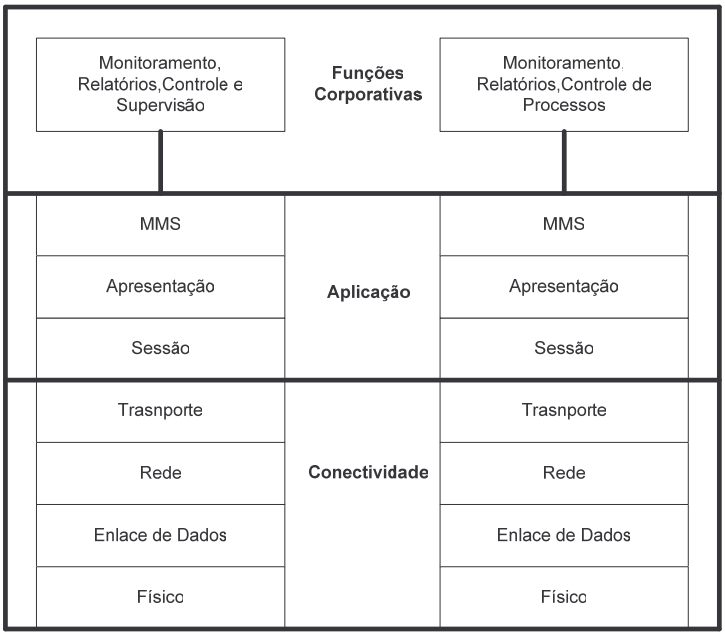


Figura 4.14 - Visão MMS de Aplicação de Rede [36].

O Barramento de Campo ou "*fieldbus*" é o termo genérico que descreve redes de comunicação de dados digital usados pela indústria [38]. Eles são utilizados para conectar dispositivos de campo, tais como, controladores, transdutores, atuadores e

sensores. São divididos em dois grandes grupos, dependendo das características que eles oferecem:

- Barramentos de Controle: Por exemplo, "*High Speed Ethernet-HSE*", ControlNet, Foundation Fieldbus, Profibus, DeviceNet, Profibus DP, SDS, Interbus-S, DNP3, MODBUS, EtherNet/IP; e
- Barramentos de Sensores: Por exemplo, CAN, ASI, Seriplex, LonWorks.

A Tabela 4.6 apresenta a família de protocolos MODBUS, MODBUS+ e MODBUS/TCP. O elemento comum em todas as arquiteturas é a estrutura cliente-servidor conhecida como "*MODBUS Application Protocol – MBAP*", um protocolo da camada 7 do modelo de referência OSI.

Tabela 4.6 - Representação da Família de Protocolos Modbus.

Modbus		**Modbus+**		**Modbus/TCP**	**OSI**
MBAP		MBAP		MBAP	Aplicação
					Apresentação
					Sessão
				TCP	Transporte
		MODICON (proprietário)		IP	Rede
RTU		HDLC		Ethernet	Enlace de Dados
EIA232	Wireless	EIA485	Fibra Ótica	Ethernet	Físico

Capítulo 5

FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

5.1 INTRODUÇÃO

Ameaças de segurança em computadores e redes de comunicação de dados tem sido um problema desde que estes recursos foram utilizados em conjunto. Em pouco tempo estas ameaças cresceram de tal forma que hoje quase todo computador e rede estão expostos a algum tipo de ameaça. Basta verificar a Figura 2.4 apresentada anteriormente para se ter uma noção deste crescimento no Brasil. Outro ponto que deve ser salientado é que a sofisticação utilizada em ataques tem aumentado sensivelmente. Isto faz com que muitas destas ameaças possam ser lançadas de forma automática, pois não é necessário nenhum conhecimento técnico. A Figura 5.1 apresenta um gráfico retirado da referência [39] que relaciona a sofisticação de ataques versus conhecimento técnico. Pesquisas usando os dados do CERT/CC nos Estados Unidos [40] indicam que esta automação pode estar sendo o gatilho para a ampliação de atividades maliciosas na Internet.

5.2 TERMINOLOGIA

Ameaça é uma pessoa, evento ou idéia que coloca em perigo uma instalação e/ou organização em termos dos objetivos de segurança. Um *ataque* é a concretização de

uma ameaça. *Proteção* ou *Salvaguarda* é um controle físico, um mecanismo, políticas ou procedimentos que protegem as instalações das ameaças. *Vulnerabilidades* são as fraquezas para uma salvaguarda ou a ausência de salvaguardas. *Risco* é uma medida da probabilidade da ocorrência de um ataque, bem como as conseqüências deste ataque. Portanto um alto risco significa uma alta probabilidade de sucesso com significantes conseqüências. As *contramedidas* são as ações que podem ser tomadas para evitar ou minimizar o risco de ataques. A *penetração ou invasão* é um ataque com sucesso, por exemplo, obter o acesso (não autorizado) a arquivos e programas ou o controle de um computador.

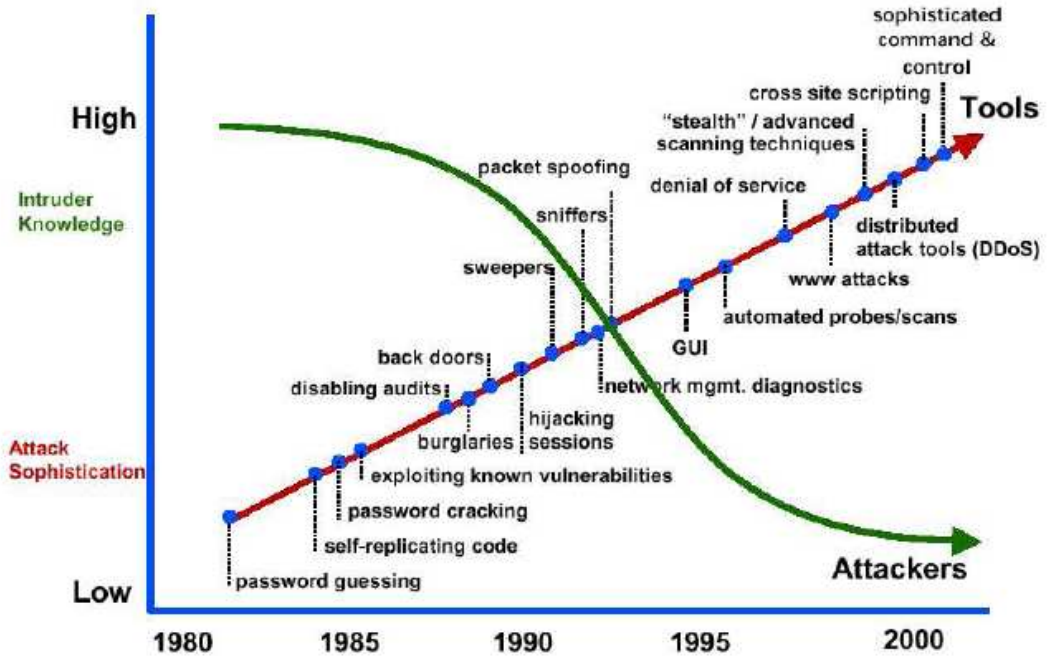


Figura 5.1 - Evolução da sofisticação de ataques versus conhecimento do atacante [39].

A Figura 5.2 mostra como a criação e o uso de ferramentas estão tornando-se cada vez mais sofisticados à medida que os invasores adotam o modelo do ciclo de desenvolvimento "*open source*", construindo e distribuindo ferramentas. As ferramentas

e as informações sobre como "quebrar" ou "penetrar" em vários sistemas, estão prontamente disponíveis na Internet, em "*bulletin boards*" e em CDs de distribuições. Mais surpreendente é o fato de que grande quantidade de informação está também disponível no software e nos manuais fornecidos para gerenciar os sistemas e as redes fornecidas diretamente pelos fabricantes.

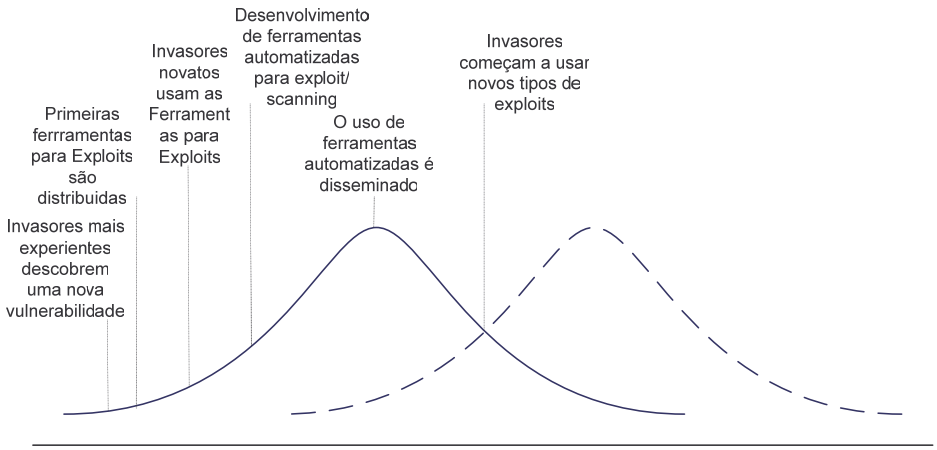


Figura 5.2 - Ciclo de exploração de uma vulnerabilidade [50].

OBJETIVOS DA SEGURANÇA DE INFORMAÇÃO

A definição da segurança para um sistema de informação, seja para a definição de uma política de segurança ou para a especificação de um sistema de informação, deve ser abordada sobre 3 perspectivas: Acesso ao Sistema de Informação, Objetivos de Segurança e Nível de Confiança no Sistema de Informação.

A primeira perspectiva diz respeito sobre como o atacante ganha acesso ao sistema de informação, se fisicamente ou por meios eletrônicos. A Tabela 5.1 resume os casos mais gerais [41]. O termo "*masqueraders*" é caracterizado por [41] como

invasores internos (Caso B). Mas [40] sugere que este termo relaciona também a invasores externos que assumiram uma identidade interna (Caso A) ou um usuário legitimo que assumiu a identidade de outro usuário por uma razão qualquer (Caso B).

Tabela 5.1 - Casos Gerais de Ameaças.

	Invasor não autorizado a usar dados/recursos do sistema	Invasor autorizado a usar dados/recursos do sistema
Invasor não autorizado a usar o computador	Caso A: Invasão Externa	
Invasor autorizado a usar o computador	Caso B: Invasão Interna	Caso C: "misfeasance"

A segunda perspectiva salienta contra que tipo de ameaça o sistema está protegido. Os objetivos de segurança descritos a seguir oferecem um quadro geral para categorizar e comparar tanto as ameaças quanto os mecanismos de segurança. São eles:

- **Confidencialidade**: Este objetivo refere-se à prevenção da divulgação de informações para pessoas não autorizadas ou sistemas.
- **Integridade**: Este objetivo refere-se à prevenção de modificações não detectadas de informação por pessoas não autorizadas ou por sistemas. Violação da integridade pode causar problemas de segurança, levando equipamentos ou pessoas a sofrerem algum tipo de dano.
- **Disponibilidade**: Disponibilidade refere-se à garantia de que pessoas não autorizadas ou sistemas não possam negar acesso ou o uso a pessoas autorizadas. Violação de disponibilidade, também conhecido como negação de serviço ("*denial-of-service – DoS*"), pode causar não somente danos econômicos mas também pode afetar a segurança, pois os operadores perdem a capacidade de monitorar e controlar o processo.

- **Autenticação**: Diz respeito com a determinação da verdadeira identidade de um usuário do sistema e o mapeamento desta identidade para um sistema interno principal, pelo qual este usuário é conhecido.
- **Autorização**: Também conhecido como controle de acesso, este objetivo diz respeito a proibição de acesso ao sistema de pessoas ou sistemas sem permissão para fazê-lo. Num sentido mais amplo, autorização refere-se ao mecanismo que distingue entre usuários legítimos e não legítimos para todos os outros objetivos de segurança. Violação deste objetivo pode produzir sérios problemas de segurança.
- **Auditabilidade**: Diz respeito com a capacidade de reconstruir o histórico completo do comportamento do sistema a partir de registros de "*log*" contendo todas as ações nele executadas. Desta forma pode-se determinar, após o incidente, o problema ocorrido e assim estabelecer extensão do incidente.
- **Não repudialidade**: Este objetivo refere-se a capacidade de fornecer provas irrefutáveis a terceiros sobre a identidade de quem iniciou uma ação em um sistema de informação. É relevante para o estabelecimento da contabilidade e responsabilidade. Violação deste objetivo trás conseqüências legais e/ou comerciais.
- **Proteção para Terceiros**: Este objetivo refere-se à capacidade de evitar danos a terceiros através do uso de um sistema de tecnologia da informação.

Alguns destes objetivos de segurança são em certos casos, independentes uns dos outros, e muitos sistemas consideram somente um subconjunto destes objetivos ou, ainda, um subconjunto como de maior prioridade.

A terceira perspectiva a ser considerada leva em consideração o nível de confiança que se pode ter de um sistema de informação em particular levando-se em conta os objetivos de segurança descritos. Este nível de confiança pode ser obtido através de certificações formais, como "*Common Criteria (CC)*", ou em termos de padrões e melhores práticas aceitas, como "*BSI Guidelines*", ITSEM, ITSEC, BS17799, COBIT, COSO, ITIL, etc. Em geral o nível de confiança nos mecanismos de segurança de um sistema diminui com o tempo, quando novos ataques e vulnerabilidades tornam-se conhecidos. Desta forma a arquitetura de segurança e sua implementação necessitam serem revistas de tempos em tempos e atualizadas quando necessárias.

5.4 O PROCESSO DE ATAQUE

Existem diversos estágios que compõem um ataque a um sistema computacional ou rede de computadores. Eles variam da motivação do atacante a execução final do ataque. Em geral classifica-se em 4 estágios principais [39]:

- Motivação do atacante e objetivo;
- Coleta de informações e seleção do objetivo;
- Seleção do ataque; e
- Execução do ataque.

Um atacante, em geral, tem várias razões para lançar um ataque. Na maioria das vezes ele simplesmente quer testar técnicas ou ainda, quer provar uma tese. Esta motivação terá impacto sobre que tipo de ataque será escolhido e como ele será executado. Antes de lançar um ataque o atacante deve selecionar o alvo do ataque e coletar informações. Estas duas atividades podem ser realizadas em paralelo ou não,

dependendo do que o atacante deseja obter. A coleta de informações envolve extrair informações úteis do computador ou da rede alvo enquanto a seleção do alvo é a escolha propriamente do objetivo do ataque. Durante estes estágios, o atacante usará ferramentas tais como "*sniffers*" e "*port scanners*" para obter estas informações. Uma vez o atacante tenha definido o alvo e obtido as informações das vulnerabilidades do alvo, ele seleciona o tipo de ataque apropriado. O estágio final é a execução do ataque, no qual o atacante lança o ataque escolhido contra o objetivo estabelecido. Em [89], uma classificação, ou taxonomia, de ataques é desenvolvida baseada no processo de ataque similar aos estágios descritos acima.

5.5 TIPOS DE ATAQUES

Dependendo da sua função específica e do ambiente, cada sistema de comunicação deve satisfazer a um subconjunto dos objetivos de segurança. Como já dito, a violação intencional de um objetivo de segurança configura-se em um ataque. Ataques podem ser iniciados a partir de pessoas de dentro da organização ou de fora da organização. Temos ainda os ataques com objetivos definidos e os ataques sem objetivo definido. Neste caso o invasor ataca qualquer sistema que apresenta uma determinada vulnerabilidade. Já o ataque com objetivo definido, o atacente tende a invadir um sistema específico com o propósito de espionagem, terrorismo ou guerra eletrônica ("*warfare*"). Normalmente este tipo de ataque é precedido de uma fase de coleta de informações acerca do objetivo-alvo, usando engenharia social, obtendo referências "*online"* ou "*offline*", ou ainda, ferramentas de verificação de vulnerabilidades em sistemas e na própria rede (como por exemplo, "*port scanners*", etc.). Em [42] encontramos uma boa descrição sobre vulnerabilidades. Em [39] encontramos uma

metodologia para classificação ("*taxonomy*") de ataques em redes e computadores. Alguns tipos de ataques mais comuns são os seguintes:

- **Denial-of-Service (DoS)**: Neste caso o atacante deseja diminuir a disponibilidade do sistema alvo, para realizar seu propósito pretendido. Para isto o ataque rompe o serviço de uma rede ou de um computador, de modo que fique impossível sua utilização ou ainda, que o desempenho da rede ou do computador seja seriamente afetado. Existem 3 tipos principais de DoS: "*host based*", "*netwok based*" e distribuído [39].
- **Eavesdropping**: O objetivo do atacante é violar a confidenciabilidade da comunicação, por exemplo, coletando indevidamente ("*siniffing*") pacotes na LAN ou interceptando transmissões em sistemas "*wireless*".
- **Man-in-the-Middle**: Neste tipo de ataque, o atacante age nos dois pontos terminais de uma comunicação (emissor-receptor), como se ele fosse o usuário esperado (parceiro) para aquela conexão. Além da violação de confidenciabilidade, este tipo de ataque permite modificar as informações trocadas, violando o objetivo da integridade. Através deste tipo de ataque, as fraquezas da implementação e o uso de certos protocolos de troca de chaves e de autenticação, podem ser explorados para obter controle de sessões criptografadas.
- **Breaking into System**: Através da violação dos objetivos de autenticação e controle de acesso, o atacante obtém a capacidade de controlar aspectos do comportamento do sistema de comunicação, incluindo a capacidade de superar os objetivos de confidencialidade e integridade. Este tipo de ataque envolve consecutivas invasões de vários subsistemas e a elevação passo a passo dos privilégios do atacante.

- **Vírus**: Ataques baseados em vírus manipulam um usuário legítimo para evitar os mecanismos de autenticação e controle de acesso a fim de executar código malicioso colocado pelo atacante. Na prática, ataques de vírus diminuem diretamente ou indiretamente a disponibilidade dos sistemas infectados através do consumo de quantidades excessivas de recursos do sistema ou da banda da rede.
- **Trojan**: É uma aplicação que se camufla como um software que não oferece perigo, mas que de fato possui uma funcionalidade maliciosa adicional. Pode ser considerado um vírus sem o componente de propagação. Uma função típica de um Trojan é fornecer um "*backdoor*" no sistema para que o atacante possa controlá-lo externamente. Também chamados de "*rootkits*", Trojans modificam partes do Sistema Operacional para impedir sua detecção. Uma versão especial de Trojans são os "*spyware*", aplicações ativas no modo "*background*" e que transmitem informações do computador infectado. Desta forma os "*trojans*" são empregados para evitar os objetivos de confidencialidade e controle de acesso.
- **Worm**: É um código malicioso cujo mecanismo de propagação é baseado na exploração de vulnerabilidades do sistema alvo, sem o envolvimento de qualquer usuário. Pode ser considerado um vírus auto-propagador, copiando a si mesmo de computador para computador via rede. Infecções por "*worm*" não tem um alvo específico e em geral cria problemas de disponibilidade para os sistemas infectados ou mesmo para a Internet como um todo. Além disso, o "*worm*" pode produzir código malicioso para lançar um ataque distribuído de todos os hosts infectados.
- **Buffer Overflow**: São extensamente usados para ataques a computadores ou a redes de computadores. Em geral fazem parte de uma combinação de ataques.

Eles são usados para explorar erros de programação, na qual "*buffers*" podem vir a ser sobre utilizados ("*overflow*"). Se um "*buffer*" é preenchido além de sua capacidade, as localizações de memória adjacentes ao "*buffer*" serão afetadas e seus dados corrompidos, ou ainda, utilizadas para modificar a execução do programa.

- **Phishing e Pharming**: É uma forma de fraude na Internet na qual os atacantes tentam enganar os consumidores para obter suas informações pessoais. As técnicas usualmente utilizadas envolvem e-mails fraudulentos e sites da web que representam e-mails e sites de web autênticos. Este tipo de ataque lança centenas ou milhares de e-mails fraudulentos, conhecido com "*spam"*, com objetivo de que uma pequena porcentagem dos consumidores responda as instruções passadas pelo atacante através do e-mail fraudulento. Estima-se que até 20% destas pessoas incautas respodam ao e-mail fraudulento, dependendo do ataque. As instituições financeiras são as maiores vitimas com grandes perdas financeiras através do uso das informações roubadas de seus clientes. Já a atividade de "*pharming*" direciona, de propósito, o usuário para sites fraudulentos ou "*proxy servers*", através de técnicas de roubo de DNS ou "*poisoning*"
- **Botnets**: O termo "*bots*" refere-se a ferramentas para tomar controle de computadores, e a coleção de computadores comprometidos pelos "*bots*" é conhecido como "*botnet*". O condutor da "*botnet*" gerencia o conjunto de computadores comprometidos (zumbis) e envia comandos dirigindo a operação da "*botnet*". O condutor pode ser ou não a pessoa que originou a "*botnet*".
- **Spoofing**: É o processo no qual o atacante passa-se por outro usuário. Neste caso um atacante pode fingir ser um usuário real ou pode manipular a comunicação

da vitima. Há várias maneiras de se realizar "spoofing" usando a pilha de protocolos TCP/IP, incluindo: "*MAC address spoofing*" e "*IP spoofing*" [39].

As tabelas 5.2, 5.3 e 5.4, obtidas no site http://www.cert.br/stats/incidentes/, apresentam os valores acumulados para os incidentes relatados ao CERT.br nos anos de 2006 e 2007(período de janeiro a junho). Fazendo-se uma análise nos valores apresentados por estas tabelas, nota-se a relativa tendência de aumento de "*worms*", se comparado o período do ano de 2006 para o primeiro semestre de 2007 (197.892 para 94.809), bem como a diminuição do número de fraudes, se comparado o primeiro semestre de 2006 com o primeiro semestre de 2007 (23.008 para 18.977 – cerca de 21%). Entretanto, o número de ataques a servidores web (aw) no mesmo período de 2006 e 2007 indica um aumento substancial de mais 160% (215 para 572). Só nos meses de janeiro a junho de 2007 aconteceram mais ataques a servidores web que no ano todo de 2006. O número de ataques de DoS diminui cerca de 27% para o mesmo período de 2006 e 2007 (253 para 199). Contudo isto não representa uma forte tendência tendo em vista o baixo número de DoS no primeiro semestre de 2007 e no segundo semestre de 2006.

Tabela 5.2: Totais Mensais no ano de 2006 Classificados por Tipo de Ataque (fonte: www.cert.br

Mês	Total	worm (%)		dos (%)		invasão (%)		aw (%)		scan (%)		fraude (%)	
jan	**8446**	1358	16	71	0	24	0	32	0	3274	38	3687	43
fev	**7742**	1223	15	33	0	59	0	54	0	2737	35	3636	46
mar	**11945**	4062	34	41	0	112	0	29	0	2925	24	4776	39
abr	**14126**	7327	51	3	0	61	0	28	0	2742	19	3965	28
mai	**18204**	11139	61	81	0	24	0	29	0	3153	17	3778	20
jun	**17470**	11036	63	24	0	44	0	43	0	3127	17	3196	18
jul	**18754**	12833	68	11	0	57	0	46	0	2823	15	2984	15
ago	**17501**	8961	51	4	0	44	0	37	0	5160	29	3295	18
set	**23321**	13499	57	4	0	26	0	38	0	5507	23	4247	18
out	**18592**	8944	48	3	0	21	0	35	0	6823	36	2766	14
nov	**23414**	16355	69	0	0	43	0	51	0	3777	16	3188	13
dez	**18377**	12939	70	2	0	8	0	27	0	3143	17	2258	12
Total	**197892**	109676	55	277	0	523	0	449	0	45191	22	41776	21

Esta análise vem demonstrar a tendência constatada pelo CERT.br da mudança de foco para o usuário final, agora vitima de "*worms*" e "*botnets*". Já o aumento de ataques a servidores web, demonstra que os provedores estão deixando muitas portas abertas para os atacantes, além de demonstrar o aumento dos relatos deste tipo de incidente ao CERT.br por parte dos provedores de serviços de web. A diminuição do número de fraudes também vai neste mesmo sentido.

Tabela 5.3: Totais Mensais no trimestre Janeiro/Março de 2007 Classificados por Tipo de Ataque (fonte: www.cert.br)

Mês	Total	worm (%)		dos (%)		invasão (%)		aw (%)		scan (%)		fraude (%)	
jan	**24181**	18109	74	0	0	8	0	21	0	3132	12	2911	12
fev	**15482**	9302	60	0	0	4	0	19	0	3907	25	2250	14
mar	**16633**	9124	54	1	0	3	0	125	0	4850	29	2530	15
Total	**56296**	36535	64	1	0	15	0	165	0	11889	21	7691	13

Tabela 5.4: Totais Mensais no trimestre Abril/Junho de 2007 Classificados por Tipo de Ataque (fonte: www.cert.br)

Mês	Total	worm (%)		dos (%)		invasão (%)		aw (%)		scan (%)		fraude (%)	
abr	**14152**	6416	45	11	0	6	0	147	1	4584	32	2988	21
mai	**13623**	5776	42	179	1	5	0	139	1	3107	22	4417	32
jun	**10738**	4621	43	8	0	15	0	121	1	2092	19	3881	36
Total	**38513**	16813	43	198	0	26	0	407	1	9783	25	11286	29

O Anti-Phishing working Group (http://www.antiphishing.org/) representa uma associação mundial composta de mais de 2600 membros, entre os quais estão oito dos maiores bancos dos EUA e mais de 1600 empresas em todo mundo. Este grupo de trabalho objetiva a eliminação das atividades de fraude e o roubo de identidade resultante das atividades criminosas de "*phishing, pharming e e-mail spoofing*". Mensalmente este grupo de trabalho divulga um relatório com as atividades de phishing a eles relatadas (http://www.antiphishing.org/reports/apwg_report_january_2007.pdf).

O gráfico da Figura 5.4 relata as atividades de janeiro de 2006 a janeiro de 2007. Segundo o relatório houve um aumento de 25% das atividades de phishing entre dezembro de 2006 e janeiro de 2007.

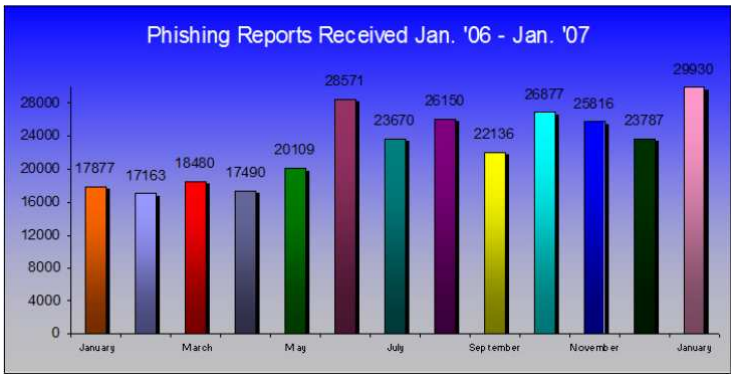


Figura 5.4 - Atividades de phishing de 2006-2007

(fonte: http://www.antiphishing.org/reports/apwg_report_january_2007.pdf)

Na Figura 5.5, outro gráfico deste mesmo relatório mostra os países que hospedam sites de phishing no mundo. EUA (com cerca de 24,27 %) e China (com cerca de 17,23 %) lideram este grupo de países . Brasil também é representado neste gráfico com cerca de 1,9 %.

Figura 5.5 - Países que hospedam sites de phishing no mundo

(Fonte: http://www.antiphishing.org/reports/apwg_report_january_2007.pdf).

5.6 MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

Segundo [34], os objetivos de segurança são obtidos através do uso de salvaguardas como "*firewalls*", Sistemas de detecção de intrusão (IDS) e protocolos de segurança presentes nas diferentes camadas das redes de comunicação. Estas salvaguardas técnicas fornecem meios para identificar usuários e controlar seus acessos aos recursos dos sistemas de informações. A Tabela 5.5, apresentada em [48], resume os mecanismos que se aplicam para o atendimento de um determinado objetivo de segurança.

O controle de conexões entre a rede interna e a internet requer, primeiramente, a definição de uma fronteira em cujos limites a organização deve controlar todos os sistemas de informações e as redes de comunicações de dados. Fora destes limites a organização tem pouco ou nenhum controle. Chamamos este limite de Perímetro de Segurança da Informação [43].

Tabela 5.5 - Qual mecanismo de segurança para qual objetivo?

Objetivo de Segurança	**Mecanismo de Segurança**
Confidencialidade	Criptografia, VPN, SSL
Integridade	Checksums criptografados, "Malware Scanners"
Disponibilidade	Redundância, Diversidade, "Malware Scanners"
Autenticação	"Pass phrases", Certificados, Tokens/Smartcards, Biometria, protocolos "chalenge-response"
Autorização	Sistemas Operacionais "endurecidos" (sem serviços inseguros ou não utilizados), contas de usuários, uso de ACLs para acesso à recursos, Firewalls, Firewalls pessoais, filtros de mensagens ao nível de aplicação, VLAN
Auditabilidade	Sistemas de Detecção de Intrusão (IDS) e logs
Não Repudialidade	Assinatura Digital
Proteção para Terceiros	Firewall e Malware Scanners

Para controlar o tráfego que atravessa o Perímetro de Segurança da Informação é colocado um "*firewall*", como na Figura 5.6. Trata-se de um equipamento ou módulo de software colocado no perímetro de segurança ou na fronteira entre as conexões de rede interna e externa, com a finalidade de protegê-la contra acessos não autorizados. Basicamente, ele examina o cabeçalho de todos os pacotes de dados de um protocolo específico que chegam e toma a decisão de admissão ou não destes pacotes. Os "*firewalls*" variam de acordo com a camada de protocolo examinada e da lógica de decisão [34].

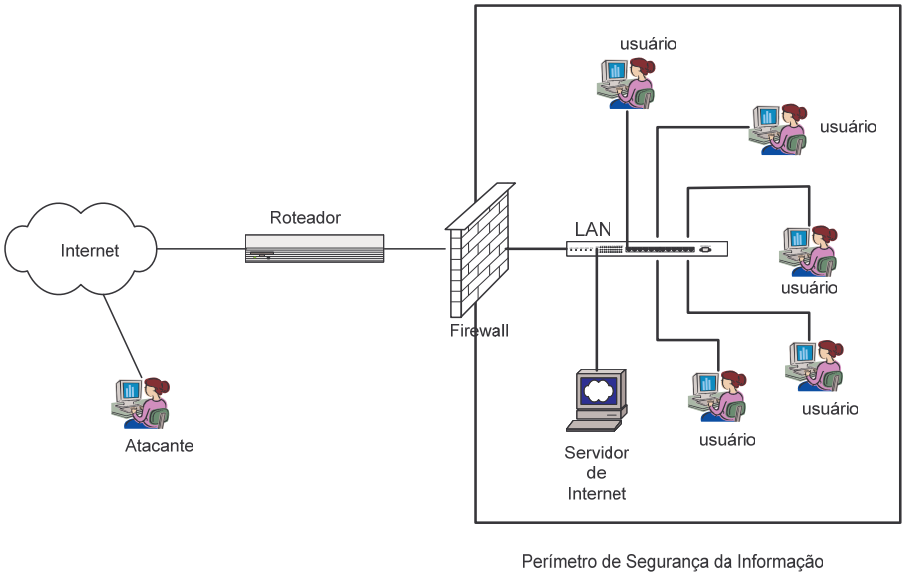


Figura 5.6 - Firewall e Perímetro de Segurança da Informação.

Outra ferramenta utilizada são os Sistemas de Detecção de Intrusão ("*Intrusion Detection Systems – IDS*"), que tentam descobrir ataques baseados em padrões conhecidos e/ou no comportamento não usual do sistema.

Os objetivos de segurança confidencialidade, integridade, autenticação e não repdudialidade são obtidos com o uso de métodos de criptografia [34]. Estes algoritmos

são utilizados para armazenagem segura dos dados e para transmissão segura dos dados. Os principais algoritmos utilizados para criptografia são:

- Algoritmos simétricos de encriptação, onde a chave de desencriptação é igual à chave de encriptação. São representados por vários algoritmos dentre os quais podemos citar o RC4, o DES, e o AES [45];
- Algoritmos com chaves públicas, onde as chaves de encriptação e desencriptação são diferentes. A chave de encriptação é pública, mas somente o receptor da mensagem que possui a chave privada correspondente poderá desencriptá-la. Os exemplos mais conhecidos são RSA e ElGamal [34]; e
- Funções de Hash, utilizadas principalmente para garantir a integridade e autenticação. As mais usadas são o MD5 e SHA [34].

A Infra-estrutura de Chaves Públicas - ICP (PKI) suporta a distribuição e a autenticação de chaves públicas. A função central é exercida pela Autoridade Certificadora (AC) que certifica um par de chaves público-privada de uma entidade geradora. A AC assina digitalmente este documento, chamado Certificado, contendo a chave pública, a informação a respeito do proprietário e a data de expiração. A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade no Brasil na cadeia de certificação. Ela está encarregada das políticas de certificação, normas técnicas e operacionais aprovadas pelo comitê-gestor da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp).

No caso dos protocolos de segurança, a ênfase é proteger a rede contra ataques nos enlaces de comunicação. Estes serviços têm como objetivo tornar seguro a comunicação entre as duas camadas pares ("*peer*") do enlace e transparente para as

outras camadas adjacentes. É possível fornecer os serviços de segurança em qualquer das quatro camadas da pilha TCP/IP. Por exemplo, quando a segurança é oferecida pela camada de rede , "*host-to-host*", todos os segmentos da camada de transporte e os dados da camada de aplicação desfrutam dos serviços de segurança da camada de rede. Contudo isto não dispensa a existência da funcionalidade de segurança nestas outras camadas. Atualmente os protocolos IPSec e SSL, das camadas de rede e de transporte, respectivamente, são os mais utilizados [34]. Na camada de enlace de dados podemos citar o protocolo IEEE802.11 utilizado para redes "*wireless*" .

A Tabela 5.6, retirada de [34], contém exemplos, divididos em camadas, dos protocolos de segurança mais comumente encontrados e os serviços que eles oferecem.

Tabela 5.6 - Protocolos de Segurança presentes em cada Camada.

Camada	Protocolo	Protocolo de Segurança	Confiden-cialidade	Integri-dade	Autenticação
Aplicação	SOAP	WS-Security	Sim	Sim	Dados de origem
	SMTP	PGP/GnuPG	Sim	Sim	mensagem
		S/MIME	Sim	Sim	mensagem
	HTTP	HTTP Digest Authentication	Não	Não	Usuário
Transporte	TCP	SSH Transport Layer Protocol	Sim	Sim	Servidor
		SSL/TLS	Sim	Sim	Servidor
Rede	IP	IPSec	Sim	Sim	Host
Enlace	PPP	CHAP/PAP	Não	Não	Cliente
	Bluetooth	Bluetooth security	Sim	Sim	Dispositivo
	WLAN IEEE802.11	WEP/WPA/802.1X	Sim	Sim	Dispositivo

5.7 SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE CONTROLE INDUSTRIAIS

Nos últimos anos tem-se visto um crescente aumento do uso de redes de computadores para transferir informações do chão de fábrica para sistemas supervisórios e corporativos, utilizando muitos dos conceitos que são aplicáveis aos sistemas de informação corporativos [54]. As tecnologias como Ethernet e TCP/IP têm sido cada vez mais utilizadas para tornar possível esta comunicação com equipamentos industriais, como em Sistemas de Controle Distribuídos (DCS) e em Controladores Lógicos Programáveis (CLP). Sistemas Operacionais como Unix, Linux e Windows também têm sido cada vez mais utilizados, juntamente com diversas aplicações populares, como planilhas eletrônicas, etc. Isto tem tornado as redes industriais menos isoladas, e portanto, mais vulneráveis, trazendo as ameaças de segurança anteriormente presentes nas redes corporativas, para as redes de controle de processos e colocando em risco tanto a produção industrial como a segurança da população [44].

Muitas destas vulnerabilidades advêm dessa necessidade de interligação dos sistemas de automação com sistemas corporativos para transferência de informações do processo industrial para fins de gerenciamento de processos e da produção e situados em níveis hierárquicos superiores. Desta forma usuários corporativos, estranhos ao processo industrial, podem acessar as informações em tempo real oriundas dos Sistemas de Controle Distribuídos (DCS) e dos Controladores Lógicos Programáveis (CLPs) e, consequentemente, passam a ter acesso a estes equipamentos anteriormente isolados da rede corporativa.

Diferentemente dos sistemas de informação corporativos que centram principalmente, seus objetivos de segurança na questão da confidencialidade e da integridade, os sistemas de controle de processos industriais têm seus principais requisitos nas questões da proteção e segurança física das pessoas e das instalações, na priorização da disponibilidade da planta industrial sobre a confidencialidade, nas restrições para resposta em tempo real e no grande tempo de vida operacional (várias décadas) dos sistemas de automação [34].

Estas diferenciações se apresentam em outros níveis, tais como requisitos de segurança e tipo de ambiente operacional, e estão muito bem analisadas em [34]. Para os sistemas de automação industrial e seus dispositivos, estas novas características criam conflitos difíceis de contornar. Por exemplo, os CLPs são dispositivos com pouco poder de processamento e com fortes requisitos para resposta em tempo real. Esta realidade pode vir a comprometer a implementação de mecanismos de segurança, como, por exemplo, os algoritmos de criptografia. Pela mesma razão, os sistemas operacionais dos dispositivos de automação não oferecem mecanismos de autenticação, controle de acesso e proteção de memória.

Byres, em [54], apresenta exemplos de problemas em redes que impactam o ambiente de produção. Segundo o autor, os problemas em redes caem em duas categorias principais: problemas acidentais ou deliberados. Os problemas deliberados são em geral causados por indivíduos com intenção maliciosa, tais como empregados descontentes e "*hackers*". Na experiência do autor, o número de erros acidentais é bem maior que o número de erros não acidentais, mas nem por isso deve-se deixar de estudá-los. O trabalho além de apresentar um estudo sobre projetos de tecnologias de redes em

ambientes industriais, apresenta um estudo de caso para implementação de política de segurança para conexão de um Sistema de Controle Distribuído (DCS) em uma rede corporativa, usando a técnica de "*access-list*" implementadas numa switch de nível 3 para filtrar pacotes oriundos da rede corporativa com destino ao Sistema de Controle, conforme mostra a Figura 5.7. Todo o tráfego que passa pela switch de roteamento (nível 3 – Camada de Rede) será filtrado, deixando passar somente as mensagens originadas nos computadores de uma determinada subnet e usando o socket 6000.

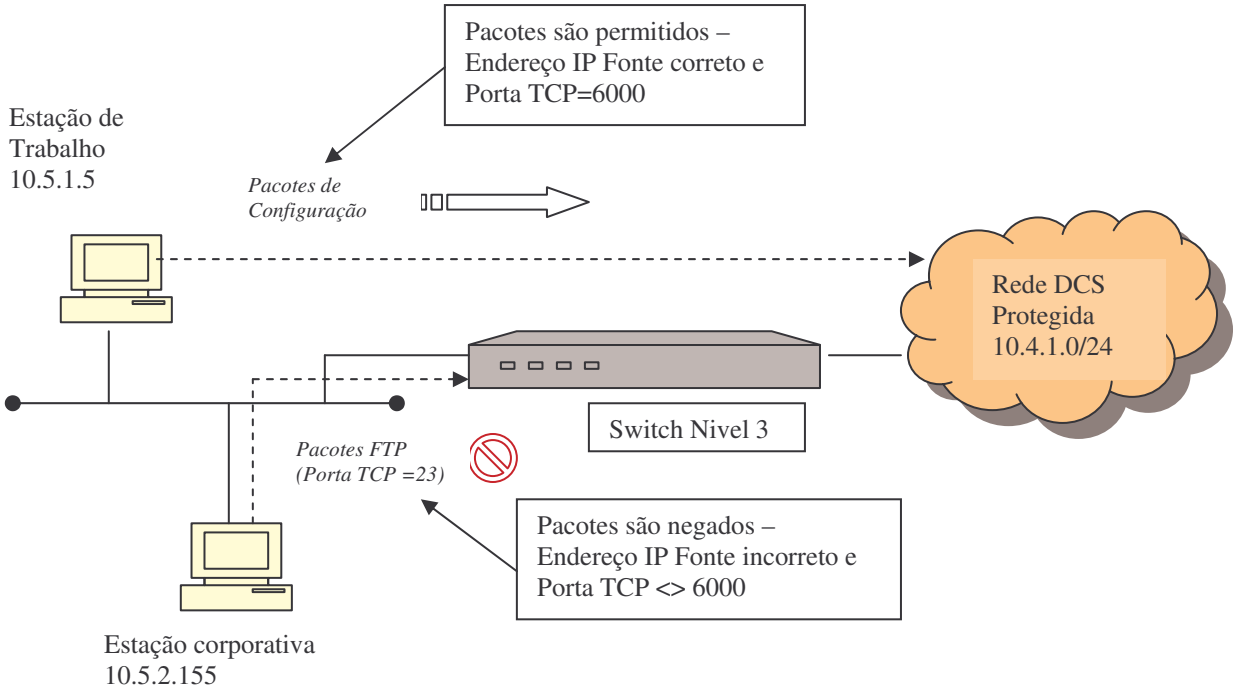


Figura 5.7 - Filtragem de Pacotes usando Switches de Roteamento com política de controle de acesso usando "*access list*"

Pela Política de Segurança estabelecida definiu-se uma regra de acesso que permite somente o tráfego da subrede 10.5.1.0/24 usando a porta 6000 entrar na rede DCS (10.4.1.0/24). Outrossim, poderia-se definir regras que permitissem que servidores específicos da sub-rede 10.4.1.0/24 do DCS acessassem a sub-rede 10.5.1.0/24, usando uma determinada faixa de número de portas. A Política de Segurança deverá, também,

definir uma regra que negue o acesso à rede DCS (10.4.1.0/24) para qualquer outro tráfego.

A Tabela 5.7, apresentada por [44], mostra a comparação feita pelos autores para as expectativas e as práticas existentes entre a tecnologia Internet e aquelas utilizadas em chão de fábrica. Fica claro que não se deve aplicar diretamente as soluções de interconexão de redes nas aplicações de chão de fábrica sem antes realizar um cuidadoso estudo no que se refere aos critérios de segurança em sistemas de controle de processos industriais.

Tabela 5.7 - Comparação entre práticas e expectativas entre as redes Internet e de Chão de Fábrica.

	Internet	**Chão de Fábrica**
Confiabilidade	Tolera falhas ocasionais; Beta teste em campo é aceitável;	Falhas são intoleráveis; Teste completo de garantia de qualidade (QA);
Impacto do Risco	Perda de Dado;	Perda de produção, equipamento e vidas;
Desempenho	Demanda alto "throughput"; Atrasos são aceitáveis;	Throughput moderado é aceitável; Grandes atrasos tornam-se grandes problemas;
Gerenciamento do Risco	Recuperação através de reboot; Segurança e proteção física de instalações e pessoas não são preocupações;	Tolerância à falhas é essencial; É necessário análise explicita de riscos;
Segurança	Muitos sites não são seguros; Pouca separação entre intranets no mesmo site; Foco é a segurança do servidor central	Forte segurança física; Rede corporativa isolada da rede de chão de fábrica; Foco é a estabilidade do dispositivo de controle;

Sistemas de automação industrial, em geral, tendem a exibir um ciclo de vida mais longo, trazendo sérias conseqüências para os sistemas legados ainda em operação e que foram projetados para trabalhar como sistemas isolados, isto é, que se baseiam no modelo que chamamos de "segurança por obscuridade" ("*security by obscurity*"). Já os novos sistemas estão sendo projetados com mecanismos de segurança, como

autenticação e controle de acesso, compatíveis com os protocolos mais modernos e devem manter-se em operação para os próximos 10 a 20 anos [34].

Em [69], o autor analisa a questão de padronização para o setor de segurança da tecnologia da informação na área industrial. O autor argumenta que para termos soluções com boa relação custo-efetividade é necessário que exista um consenso da indústria ou uma padronização. O artigo examina os interesses de vários setores no campo da segurança industrial e avalia algumas das iniciativas mais visíveis (ISA, NERC e IEC) com respeito aos benefícios e requisitos para estes setores. Também apresenta um detalhamento do "*draft*" do grupo de trabalho em segurança de sistemas de controle industrial dentro da norma "*IECTC65 – Digital communications*".

Em [70], os autores descrevem a aplicação da "*NIST Special Publication 800-53-Recommended Security Controls for Federal Information Systems*" para Sistemas de Controle Industriais. Trata-se de uma iniciativa do "*Industrial Control System Security Project*" estabelecido pelo "*National Institute of Standards and Technology – NIST*", para melhorar a segurança de sistemas de controle industriais do setor público e privado. O artigo tem o foco na comparação da SP 800-53 [71] com o "*NERC CIP Standards – CIP -002-1 to CIP-002-9*" [29]. Nos EUA, as agências federais que possuam, operem e mantenham sistemas de controle industriais devem estar de acordo com os padrões de segurança da informação do NIST.

Como parte das iniciativas do "*ICS Project*", o NIST publicou em Dezembro de 2006 o "*Draft SP 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*" [72]. Este documento é um guia para estabelecer sistemas de controle industriais seguros, incluindo sistemas SCADA,

Sistemas de Controle Distribuído e outros sistemas de controle de menor porte, usando CLPs. O documento descreve sistemas de controle industriais e suas topologias típicas, identifica as ameaças e as vulnerabilidades destes sistemas e fornece contramedidas de segurança recomendadas para mitigar os riscos associados.

Naedele, em [62], relaciona de forma muito clara os problemas anteriormente mencionados para segurança em sistemas de controle industriais e discute suas possíveis soluções. Ele argumenta que o principal obstáculo à segurança em sistemas de controle não é técnico, mas financeiro. O artigo divide os problemas encontrados em 4 grandes categorias. Para cada problema ou desafio, como ele prefere referenciar, ele apresenta um elenco de soluções. A seguir apresenta-se uma breve citação destes desafios, pois fornece as direções para futuras pesquisas:

- Desafios organizacionais e de percepção do problema: Segurança não deve ser visto somente pelo aspecto técnico, mas relacionado ao comportamento humano e a percepção do problema. Os pontos em discussão devem ser:
    - Definição de Política;
    - Distribuição não clara da responsabilidade da segurança de sistemas de controle entre as áreas de TI corporativo e a operação do processo;
    - Conscientização sobre os riscos de conexões externas;
    - Conscientização do risco de ser atacado;
    - Confiança na segurança por obscuridade;
    - Confiança em medidas regulatórias;
    - Confiança em certificações;
- Desafios em relação ao tempo de vida operacional do sistema de controle industrial: Relacionados com o longo tempo de vida operacional dos

sistemas de controle. Isto significa que os sistemas projetados e implementados atualmente não estão levando em conta as questões de segurança em seus projetos:

  - Sistema de controle sem mecanismos de segurança;
  - Sistemas de controle que não podem ser atualizados/ "*patched*";
  - Tempo de vida operacional de componentes "*commercial-off-the-shelf - COTS*";
  - Mecanismos de segurança que necessitam serem continuamente atualizados;
  - Protocolos de comunicação sem mecanismos de segurança;

- Desafios técnicos: Relacionados com tecnologia e os requisitos operacionais para sistemas de controle:
  - Necessidade de poder computacional;
  - Latência induzida pela proteção criptográfica;
  - "*Scanning*" intrusivo de vulnerabilidades;
  - Impedir "*Malware*";
  - Impedir entrada de requisições;
  - Tratamento da Emergência como prioridade mais alta que segurança/controle de acesso;
  - Detecção de intrusão em sistemas de automação;
  - Controlar acesso remoto para clientes;
  - Utilizar Tecnologias de comunicação sem fio segura;
- Desafios financeiros: Manter sistemas de controle seguros levando-se em conta o nível de custo aceitável pelo proprietário do sistema.

Em resumo, propostas para novos mecanismos de segurança não devem ser avaliados somente sob a perspectiva de aumento de custos. Isto posto, as pesquisas neste campo deveriam concentrar em tornar o tópico segurança para sistemas de controle com uma melhor relação custo-efetividade.

Capítulo 6

AMEAÇAS E VULNERABILIDADES EM SISTEMAS ELÉTRICOS DE POTÊNCIA

O setor de energia elétrica pode ser considerado como parte da infra-estrutura crítica de qualquer nação. O objetivo neste item é descrever sucintamente esta infra-estrutura e relatar suas vulnerabilidades.

6.1 TIPOS DE SISTEMAS DE INFORMAÇÃO

Os sistemas de informação de uma empresa de energia elétrica em geral são divididos em 4 grandes grupos de sistemas computacionais [76]:

- Sistema Computacional Corporativo: Realiza funções de gerenciamento do negócio, contabilidade e cobrança. Não é utilizado na operação do sistema, mas atualmente, seguindo a tendência, tem-se investido no aumento esta conectividade.
- Sistema Computacional para Engenharia: Compreende os sistemas que mantém dados para a coordenação do planejamento, projeto e operação do sistema interligado.

- Sistema Computacional para Centros de Controle: Compreende os sistemas EMS -"*Energy Management System*" e SCADA – "*Supervisory Control Data Acquisition System*".
- Sistema Computacional Embarcado: Compreende os equipamentos de controle, muitos deles baseado em microprocessadores, tais como UTRs, IEDs, etc. Estão localizados nas subestações remotas e semi-assistidas ou totalmente não assistidas e unidades de geração.

Voltando ao conceito das camadas que compõe o domínio da infra-estrutura crítica do setor elétrico, a camada cibernética é composta de diversos centros de controle, software de gerenciamento de energia (EMS), aplicativos e bancos de dados conectados através de redes de comunicação de dados. Estes centros de controle interagem com sistemas SCADA, que por sua vez fazem a interface com as Unidades de Terminais Remotas (UTRs) os quais monitoram sensores, disjuntores, transformadores, linhas e transmissão e unidades geradoras, os quais formam a camada física.

A camada de operação contém as interfaces homem-máquina (IHM). A Figura 6.1 representa o diagrama em blocos de um típico centro de controle. Pode-se constatar que a chave da operação em tempo real do sistema elétrico depende da infra-estrutura de comunicações composta pelas redes de comunicações de dados internas e externas da organização.

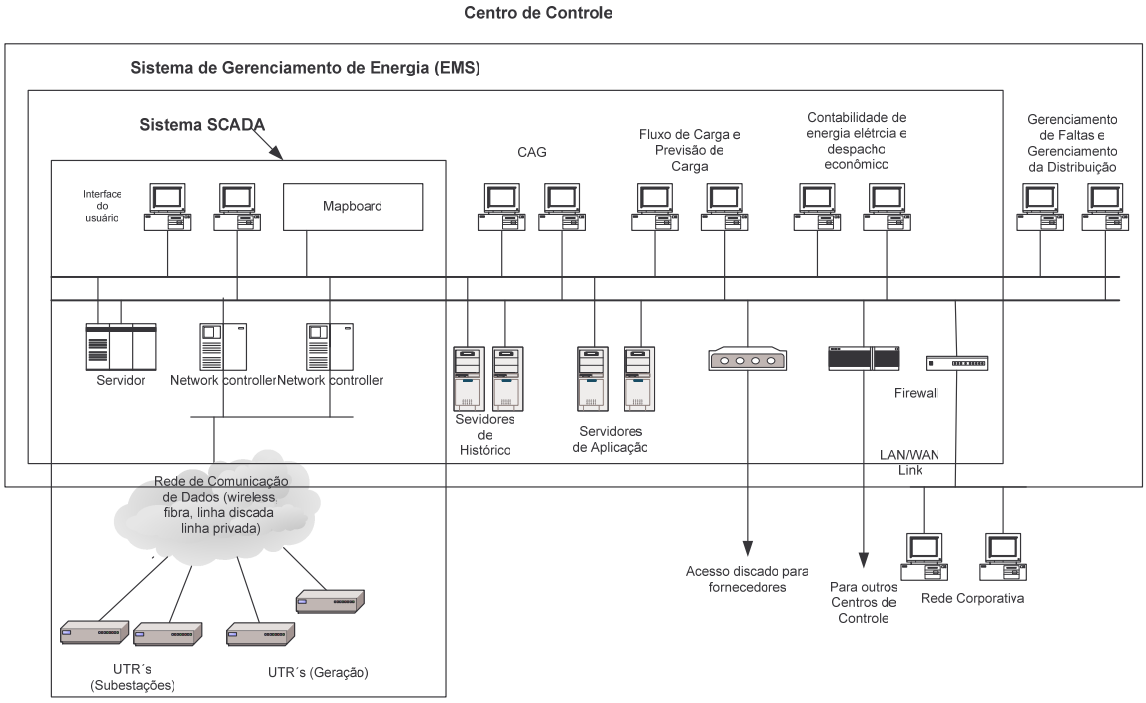


Figura 6.1 - Diagrama de Blocos de um Centro de Controle [53].

Já a Figura 6.2 mostra um diagrama típico da infra-estrutura de telecomunicações do setor elétrico. Tradicionalmente, esta infra-estrutura era protegida pelo seu relativo isolamento e pela utilização de protocolos não padronizados ("*security by obscurity*"). Contudo as mudanças no mercado de energia elétrica quem têm ocorrido no mundo todo, não mais comportam tal isolamento, levando as organizações do setor de energia elétrica a cada vez mais fazer uso de tecnologias que permitam uma maior interconectividade. A diversidade funcional destas organizações tem resultado na necessidade da utilização de sistemas abertos, não proprietários, de tal forma a permitir cada vez mais à integração com outros sistemas, internos ou externos a organização [43]. Além dos problemas ligados ao crescente uso dos protocolos TCP/IP, os sistemas SCADA também estão sujeitos a suas próprias vulnerabilidades. Por exemplo, um invasor poderia conectar-se diretamente a dispositivos eletrônicos inteligentes (IEDs) utilizando-se de linha telefônica pública e abrir disjuntores ou realizar algum outro tipo

de ação maliciosa. Outra possibilidade seria que uma falha ou ataque poderia alterar a visão do operador do sistema interligado, levando-o a tomar ações incorretas com conseqüências desastrosas. Exemplos de ocorrências e ações maliciosas em sistemas elétricos de potência e outras concessionárias de serviços públicos são referenciados em [26, 30, 46, 47, 48]. Em [53], encontramos uma extensa lista de eventos ocorridos desde 1945 até 2003.

Portanto o principal problema no gerenciamento de redes de comunicações de dados em sistemas elétricos atualmente é o impacto dos ataques e acidentes cibernéticos no monitoramento e no controle do sistema interligado.

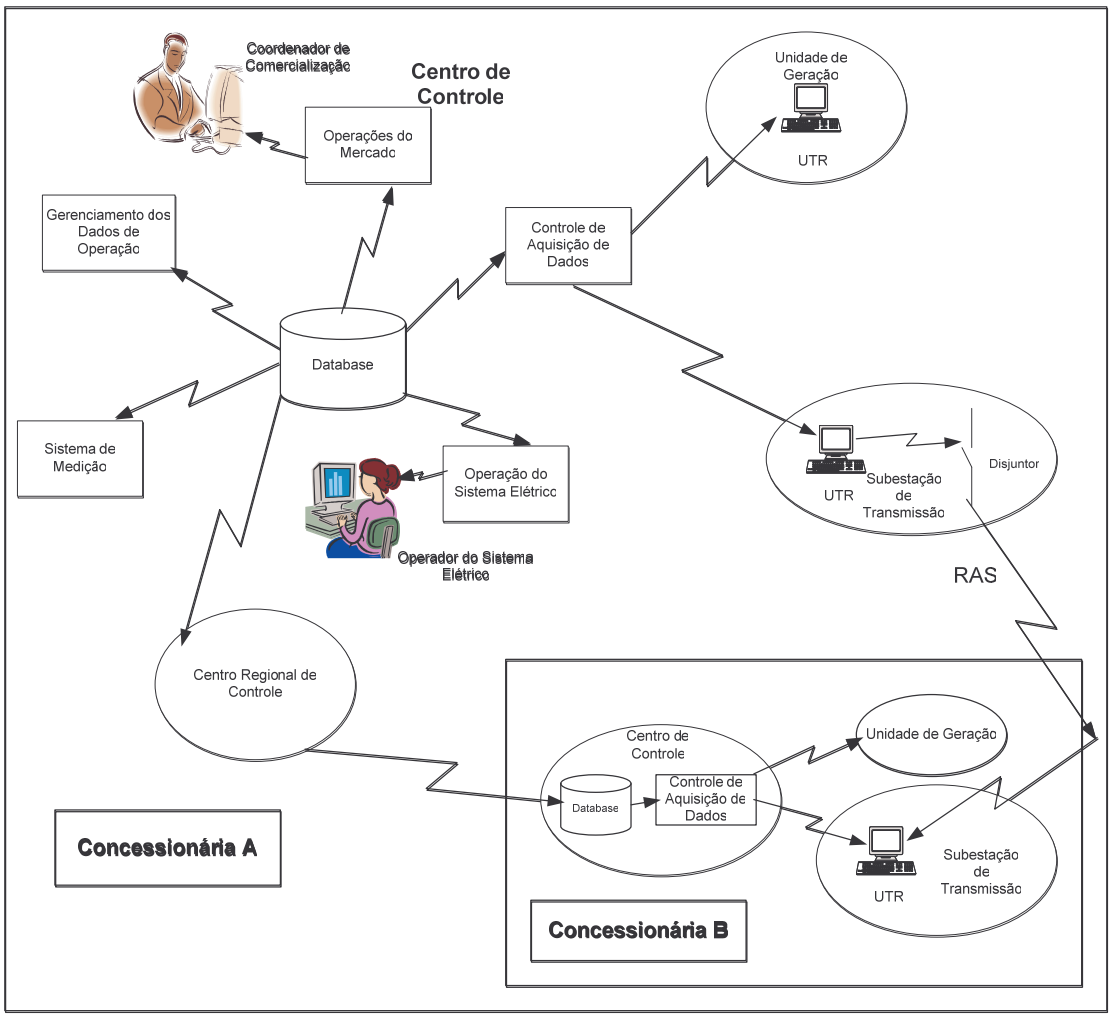


Figura 6.2 - Típica Infra-estrutura de comunicações para sistema elétrico [55].

A referência [78] indica que o ponto central do problema de segurança em sistemas SCADA reside em três erros de conceito que são comumente feitos pelos gerentes de empresas do setor elétrico:

- Sistemas SCADA residem em redes fisicamente separadas e isoladas;
- Conexões entre sistemas SCADA e outras redes corporativas são protegidas por fortes controles de acesso;
- Sistemas SCADA necessitam de conhecimentos especializados, tornando-os difíceis para invasores de rede acessar e controlar.

Como resultado destes conceitos errôneos, os sistemas SCADA têm-se tornado ainda mais vulneráveis a ataques às suas redes internas e externas. Com a pressão da desregulamentação do setor, forçando a adoção de novas tecnologias de TI, estas vulnerabilidades têm aumentado mais rapidamente.

A referência [73] faz uma revisão de alguns dos riscos e vulnerabilidades que os atuais sistemas elétricos de potência estão enfrentando e examina soluções e iniciativas propostas nos EUA, Chile e Brasil. O autor alega que os riscos de segurança cibernética atualmente são maiores que os riscos físicos. Ele aborda, também, o Plano de Defesa do Sistema Interligado Brasileiro, desenvolvido pelo CEPEL, Eletrobrás e ONS, e o considera um plano revolucionário.

A referência [6] sugere que é necessário que se crie um sistema capaz de avaliar a confiabilidade dos dados oriundos do sistema elétrico de tal forma a produzir uma resposta rápida quando necessário.

A referência [55] alega que a atual infra-estrutura de comunicações para o setor elétrico é inadequada em razão de que tal infra-estrutura foi desenvolvida durante as últimas décadas em função de um mercado de energia elétrica regulado, diferentemente da realidade atual. Esta infra-estrutura é centrada na comunicação entre centros de controle e subestações usando topologia de rede em estrela e com o sistema SCADA transferindo informações de status e comando dentro de um intervalo de tempo de vários segundos, conforme mostrado anteriormente na Figura 6.2. Os autores propuseram, então, uma nova infra-estrutura de comunicações e controle, conhecida como GridStat, descrito em [56, 57, 58], para transmitir informação de status, dados representando fenômenos operacionais dinâmicos, como tensão, corrente e status de disjuntores além de comandos de decisão. GridStat é implementado como "*middleware*", um software de alto nível no topo do sistema operacional, tornando mais simples a tarefa de criação de aplicações de computação distribuída. Outro modelo de referência para sistemas de controle e automação em sistemas elétricos foi desenvolvido pelo Sandia National Laboratories [60]. Os autores alegam que as infra-estruturas dos sistemas de automação estão cada vez mais expostos às ameaças cibernéticas em função da maior visibilidade e do aumento do uso de modernos componentes de tecnologias da informação. O artigo introduz um modelo de referência baseado na modelagem por objetos e desenvolve conceitos fundamentais para a segurança baseada na análise do modelo. O modelo proposto para um sistema de automação de energia elétrica é apresentado. Outras iniciativas, como "*IntelliGrid Architecture*", podem ser encontradas em [51] e [63].

A referência [79] sugere outro modelo para o estudo e a análise de segurança de um sistema elétrico integrado como um todo. Como a tendência atual é de que os

sistemas de controle e os sistemas corporativos cada vez se integrem/interconectem mais e mais, o modelo tradicional de descrever e analisar redes de computadores sob a perspectiva de hardware, isto é, em termos de servidores, roteadores, bridges/switches, etc, não é mais válida. Os autores trabalham com o conceito de domínios de segurança, isto é, uma área específica onde as atividades/operações do negócio estão ocorrendo e podem ser agrupados. Os domínios identificados pelos autores são:

- Domínio Público, do Fornecedor, da Mantenedora;
- Domínio da Geração;
- Domínio da Subestação;
- Domínio das Telecomunicações;
- Domínio das operações em tempo real; e
- Domínio do Sistema de Informação Corporativo.

Figura 6.3 - Domínios de Segurança.

O artigo define e descreve cada domínio de segurança e suas inter-relações e finaliza apresentando como a segurança da informação pode ser gerenciada baseando-se na norma internacional ISO/IEC 17799. Após a identificação dos requisitos de segurança da informação, controles devem ser selecionados e implementados para garantir que os riscos serão reduzidos a um nível aceitável. Dependendo do domínio de segurança definido, controles devem ser selecionados da norma ISO/IEC17799 e adaptados para as necessidades das empresas do setor elétrico. Novos controles devem ser projetados para atender as necessidades específicas. Grupos como ISA e IEC, estão trabalhando no desenvolvimento de políticas e procedimentos genéricos [69]. Este é o esforço resultante do Cigré Joint Working Group (JWG) D2/B3/C2-01 "*Security for Information Systems and Intranets in Electric Power Systems*".

6.2 SISTEMA ELÉTRICO DE POTÊNCIA

A estrutura básica do sistema elétrico de potência consiste dos sistemas de geração, transmissão, distribuição e centros de controle. A energia elétrica gerada pelo sistema é transformada para tensões mais elevadas para uma maior eficiência na transmissão em longas distâncias. A interconexão destes sistemas de transmissão forma a "grade de potência" ("*power grid*"), que permite a troca de energia elétrica entre diversas empresas do setor de energia elétrica. As linhas de transmissão terminam em subestações, onde a tensão é reduzida para os níveis de tensão de distribuição primária. Esta tensão é então fornecida diretamente para os clientes industriais, ou sofre novo processo de transformação e é rebaixada para a distribuição local. A Figura 6.4 mostra esta estrutura.

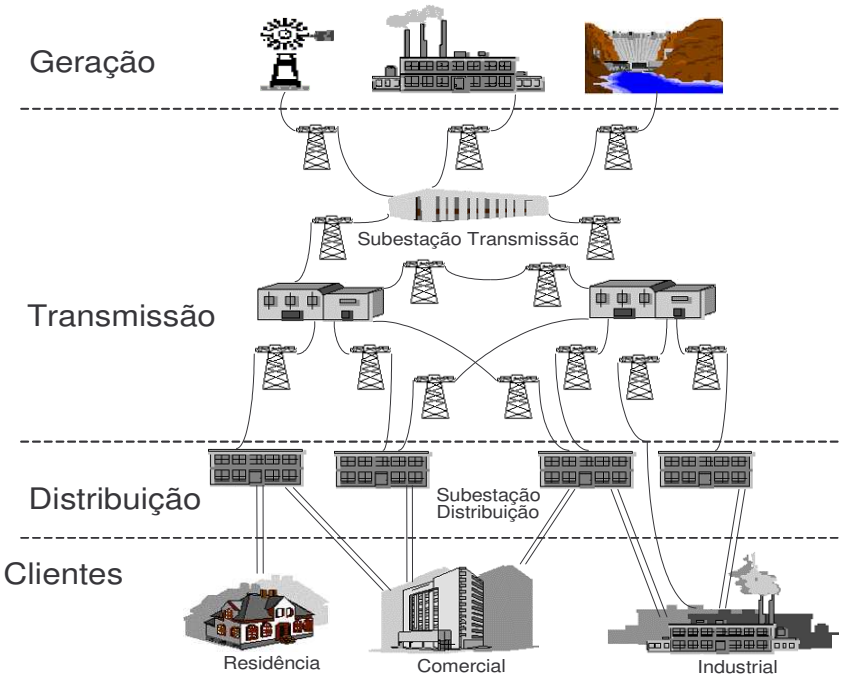


Figura 6.4 - Sistema Elétrico de Potência [52].

6.2.1 Centros de Controle

Os centros de controle monitoram/controlam as unidades de geração, transmissão, distribuição e as cargas dos clientes. A sua função primária é fornecer o monitoramento centralizado das operações do sistema elétrico de potência, coordenar e otimizar a geração e a transmissão de energia, manter dados históricos e permitir o controle manual e automático dos equipamentos em campo. Os dados coletados pelos centros de controle podem ser visualizados através de interface gráfica permitindo que os operadores possam intervir em vários pontos de controle do sistema elétrico de potência. Estas funções são realizadas pelos Sistemas de Gerenciamento de Energia (EMS). A Figura 6.1, apresentada anteriormente, mostra uma configuração típica de um Centro de Controle e as interfaces com o Sistema de Gerenciamento de Energia (EMS).

As operações de controle de um sistema elétrico de potência interligado podem ser divididas, segundo [57] e [58], em:

- Controle local: São aqueles que usam entradas que são geradas localmente na subestação em que as saídas de controle serão aplicadas. As entradas são usualmente valores analógicos, tais como tensão, corrente, potência ativa e reativa, e as saídas de controle são valores digitais (abrir/fechar) ou parâmetros discretos, como taps de transformadores, ou contínuos, como o regulador de tensão de um gerador. São exemplos de sistemas de controle local o sistema de Controle da Proteção do Sistema, o sistema Controle do Regulador de Velocidade do Gerador, o sistema de Controle de Tensão e o sistema de Controle do Fluxo de Potência ("*Power System Stabilizers"- PSS*). A característica em comum destes sistemas de controle é que são rápidos e não exigem enlaces de comunicação de longa distância. O sistema de controle da proteção do sistema desempenha função primordial, pois protege os equipamentos elétricos de faltas. Como são baseados em microprocessadores, possuem tempo de resposta rápido (cerca de 2 a 3 ciclos) e seus parâmetros de gatilhamento são locais. Novas tecnologias, utilizando eletrônica de potência, estão sendo utilizadas, como FACTS ("*Flexible AC Transmission Systems*") e SVC (Compensadores Estáticos), tornando mais rápido o tempo de resposta destes sistemas.
- Controle geograficamente espalhado: Este é o caso onde o sistema de controle necessita de enlaces de comunicação para coletar dados ou enviar sinais de controle. São exemplos o Controle de Freqüência, o sistema de Controle de tensão secundário (regional) e "*Special Protection Schemes (SPS) / Remedial Action Schemes (RAS)*". O Controle de Freqüência se baseia no principio de que

a freqüência se desviará do parâmetro nominal sempre que haja um desbalanço entre a geração e a carga. Ele e é dividido em 2 partes: o controle primário, local a unidade geradora e um laço de controle secundário, denominado Controle Automático de Geração - CAG - que coordena os sinais das várias unidades que compõem este laço de controle. O Centro de Controle coleta as freqüências relevantes do sistema e a informação do fluxo de potência e envia os pontos de ajuste para cada unidade participante do CAG. O tempo para envio de comandos do CAG varia entre países, sendo 2-4 segundos nos EUA [58] e no Brasil [59]. Alguns países começam a implementar, também, o controle de tensão secundária (regional), principalmente na Europa. Este esquema, análogo ao controle de freqüência, monitora a tensão nos principais barramentos e organiza as tensões em uma grande área para manter a tensão do barramento principal. Estes pontos de ajuste de tensão são então despachados para os controladores locais. Já os sistemas SPS/RAS são esquemas altamente especializados que respondem ajustando equipamentos remotos no caso de alguma falta ou outro evento. O uso de SPS/RAS está aumentando em sistemas com estabilidade limitada onde a disponibilidade de tais esquemas permite a transferência de energia que poderia provocar instabilidade devido a certos tipos de faltas. Tais esquemas são inflexíveis e "*hardwired*" e se baseiam na existência de enlaces dedicados de comunicação e com um grande poder de cálculo dos parâmetros "*offline*". Conforme [74], um esquema SPS baseado em CLPs, chamado de "Controle de Segurança" o qual introduz o conceito de Zonas de Segurança e Matriz de Segurança da Rede, foi adotado para melhorar a segurança do Sistema Interligado Nacional, permitindo tempo de resposta de 200 ms no atendimento de mudanças topológicas da rede, pois a troca de

informações dentro de uma zona de segurança e entre zonas vizinhas deve ser rápido, organizado e confiável para garantir a operação adequada da lógica do SPS. Desta forma este esquema é altamente dependente de uma efetiva rede de comunicações

O Sistema de Gerenciamento de Energia do Centro de Controle incorpora o Banco de Dados do Sistema, Aplicações Operacionais e para a Visualização, bem como a função de Geração de Relatórios do Sistema. A necessidade de disseminar dados específicos do sistema elétrico dentro da empresa concessionária, facilitando seu compartilhamento entre os diversos departamentos, tem resultado na conexão dos sistemas EMS à rede corporativa (LAN ou WAN).

Em geral as comunicações entre o centro de controle e os equipamentos de campo são feitas através de enlaces de comunicação mantidos pela própria empresa. A grande maioria utiliza enlaces de microondas, embora a fibra ótica também seja muito utilizada através dos cabos OPGW. Outros meios de comunicação incluem linhas dedicadas alugadas, carrier, satélite e rádio.

O EMS em geral consiste das seguintes aplicações:

- Sistema de Controle Supervisório e Aquisição de Dados (SCADA);
- Controle Automático de Geração (CAG);
- Aplicações de gerenciamento de energia, tais como previsão de carga, despacho econômico, fluxo de carga, contabilidade de energia, controle de tensão/VAR e Banco de Dados, dentre outras; e
- Sistema de Interface Homem-Máquina (IHM).

6.2.2 Sistema SCADA

O sistema SCADA pode ser visto como uma coleção de componentes distribuídos que fornece as seguintes funções básicas para realizar o controle e o monitoramento de um sistema:

- Medição – Geração de dados.
- Aquisição de Dados – Coleta de Dados.
- Controle – Validação dos dados, geração da informação, determinação da resposta e resposta automática ou manual.
- Interface Homem-Máquina (IHM) - Processa as entradas e apresenta as informações para os operadores.

O sistema consiste de um ou mais computadores executando aplicações específicas do setor elétrico em tempo real e conectado através de uma rede de comunicação de dados a várias unidades remotas localizadas em diversas localizações com a função de coletar dados, realizar o controle inteligente dos dispositivos do sistema elétrico e relatar ao EMS, conforme mostrado na Figura 6.1. Para tanto, o sistema SCADA mantém enlaces de comunicação em tempo real com o EMS do Centro de Controle e entre várias subestações.

Da Figura 6.2, apresentada anteriormente, verifica-se que o Sistema SCADA tem múltiplas conexões de rede. Estas conexões podem ser divididas em “internas” e “externas”. Conexões internas referem-se a conexões dentro do sistema, enquanto conexões externas referem-se a conexões entre sistemas SCADA ou EMS. Em geral o meio físico usado para criar estas conexões consiste tipicamente de modem, linhas

alugadas, fibra ótica, "*wireless*" (microondas ou "*spread spectrum radio*") e enlaces de satélites. O protocolo mais popular dentro de uma subestação é o "*Distributed Network Protocol*" (DNP) 3.0. Para conexões a redes externas, o protocolo mais popular é o "*Intercontrol Center Communication Protocol*" (ICCP) [61].

Não existe um padrão único que cubra todos os sistemas SCADA. Contudo, existem muitos padrões adicionais que discutem componentes de hardware e software específicos de sistemas SCADA. A Tabela 6.1, retirada de [61], apresenta alguns destes padrões mais conhecidos.

Tabela 6.1 - Padrões relacionados a sistemas SCADA

Padrão	Titulo	Descrição
ANSI C37.1	Padrão IEEE para definição, especificação e análise de sistemas usados para controle supervisório, aquisição de dados e controle automático	Contém definições e características importantes para sistemas SCADA
IEEE 802.3	Padrão para troca de informações entre redes locais e redes Campus. Define o método de acesso CSMA/CD e as especificações da camada física	Padrão descreve requisitos para Ethernet usando par trançado (10BaseT)
IEEE 999	Prática recomendada pelo IEEE para sistemas SCADA Master/Remote	Estabelece práticas recomendadas e protocolos de comunicação entre estações master e remote
IEEE 1379	Prática recomendada para comunicação de dados entre UTRs e IEDs numa subestação	Fornece recomendações para implementação dos protocolos DNP3.0 e IEC60870-5-101 em subestações
IEEE 1402	Guia para segurança eletrônica e física em subestações	Fornece recomendações para segurança eletrônica e física em subestações
IEC60870-5	Equipamentos e Sistemas de telecontrole – Parte 5-101: Protocolos de Transmissão	Descreve versão serial e de rede do protocolo no qual DNP3.0 é baseado
IEC60870-6	Equipamentos e Sistemas de Telecontrole – Parte 6: protocolos de telecontrole compatíveis com padrão ISO e recomendações ITU-T	Descreve o protocolo TASE.2(também referenciado como ICCP)
IEC61850	Redes e sistemas de comunicação em subestações	Descreve protocolo similar a UCA 2.0

A referência [77] enumera 21 passos para melhorar a segurança eletrônica de redes SCADA. Este documento foi elaborado por iniciativa do "*Office of Energy Assurance*" do Departamento de Energia dos EUA em resposta ao "*President's Critical Infrastructure Protection Board*" de Outubro de 2001. Cada passo focaliza ações

específicas a serem tomadas para aumentar a segurança de redes SCADA e minimizar as vulnerabilidades:

- Identificar todas as conexões para Redes SCADA;
- Desconectar conexões consideradas desnecessárias para redes SCADA;
- Avaliar a segurança das conexões remanescentes;
- "Endurecer" redes SCADA, desabilitando ou removendo serviços desnecessários;
- Não confiar em protocolos proprietários para proteção do sistema;
- Implementar as características de segurança fornecidas pelo fabricante do dispositivo;
- Estabelecer controles de acesso para qualquer meio que possa ser usado como "*backdoor*" para a rede SCADA;
- Implementar detecção de intrusão interna e externa e estabelecer monitoramento de incidentes 24 horas por dia;
- Realizar auditorias técnicas em dispositivos e redes SCADA e qualquer outra rede conectada para identificar vulnerabilidades;
- Realizar avaliação de segurança física em todos os "sites" remotos conectados a rede SCADA para avaliar segurança;
- Estabelecer equipes ("*red teams*") para avaliar e identificar possíveis cenários de ataques;
- Definir claramente as funções de segurança, responsabilidade e autoridade para gerentes, administradores de sistemas e usuários;
- Documentar a arquitetura da rede e identificar sistemas críticos ou que contenham informações classificadas;
- Estabelecer um rigoroso processo de gerenciamento de risco;

- Estabelecer estratégias de proteção de redes baseados no princípio "*defense-in-depth*";
- Identificar claramente os requisitos de segurança cibernética;
- Estabelecer processo de gerenciamento efetivo de configuração;
- Conduzir auto-avaliações rotineiras;
- Estabelecer "*backups*" do sistema e planejamento de recuperação de desastres;
- A liderança organizacional deve estabelecer as expectativas para o desempenho da segurança cibernética; e
- Estabelecer políticas e realizar treinamentos para minimizar a probabilidade que pessoal da organização divulgue inadvertidamente informações classificadas sobre o projeto do sistema SCADA, a operação e os controles da segurança dos sistemas.

A referência [119] identifica ameaças enfrentadas por sistemas SCADA e investiga os métodos mais eficazes para melhorar a segurança destes produtos analisando o protocolo DNP3, que tem se tornado um protocolo padrão *de facto* para a indústria na implementação dos sistemas de comunicação em sistemas SCADA. Os autores propõem alternativas com uma boa relação custo/efetividade incluindo SSL/TLS, IPSec, segurança por objetos, criptografia e autenticação de mensagens. O documento avalia detalhes da implementação destas soluções, analisa e compara estes modelos. Os autores sugerem, ainda, novas direções para as pesquisas que busquem melhorias na segurança de sistemas SCADA por um longo período de tempo.

6.2.3 Unidades de Terminais Remotas (UTR)

As UTRs são computadores de propósito especial baseados em microprocessador que contém conversores analógico para digital (ADC), conversores digital para analógico (DAC) e entradas/saídas digitais utilizadas para informação de status e controle. Estas unidades são utilizadas em diversos pontos das subestações e das unidades de geração para controlar e monitorar diversos tipos de equipamentos. Podem ter centenas de enlaces de comunicação em tempo real com outras subestações, com o EMS do Centro de Controle e com as unidades de geração. Desta forma podem ser configuradas e controladas à distância.

6.2.4 Controladores Lógicos Programáveis (CLP)

Desde há muito tempo o CLP é extensivamente utilizado nas indústrias de manufatura e de processos. Agora estão sendo também utilizados para a implementação de relés e sistemas de controle em subestações. As saídas de controle são controladas por software residindo no CLP ou via comandos remotos do Sistema SCADA. O usuário poderá fazer mudanças no software armazenado em EEPROM sem necessidade de grandes mudanças no hardware ou no software. Os CLPs mantêm enlaces de comunicação em tempo real, internamente e externamente, com subestações e unidades de geração.

6.2.5 Relés de Proteção

Os relés de proteção são projetados para responder a faltas do sistema, como por exemplo, curto-circuito. Quando uma falta ocorre, o relé deve sinalizar ao disjuntor apropriado para ativar e isolar o equipamento com falta. Sistema de relés em linhas de transmissão deve localizar e isolar a falta com velocidade suficiente para preservar a

estabilidade, reduzir o dano e minimizar o impacto no sistema elétrico de potência. Certos tipos de relés inteligentes podem ser configurados e inspecionados usando redes de comunicação de dados.

6.2.6 Medição Automatizada

A medição automatizada é projetada para realizar o "*upload*" de dados da medição de consumo de energia elétrica de estabelecimentos residenciais ou comerciais. Estes dados serão automaticamente descarregados em um dispositivo dedicado e transmitidos para o ponto de coleta central. A questão aberta, neste caso, é que com esta tecnologia os enlaces de comunicação em tempo real externos ao sistema elétrico de potência passarão a coexistir com a infra-estrutura. Na Figura 6.5 apresentamos um diagrama exemplo deste tipo de medição automatizada. Trata-se da arquitetura do Sistema de Coleta de Dados de Energia (SCDE), implantado e mantido pela Câmara de Comercialização de Energia Elétrica (CCEE), conforme resolução ANEEL No. 109 de 26-10-2004, e que visa viabilizar a coleta dos dados de energia elétrica para uso no Sistema de Contabilização e Liquidação (http://www.ccee.org.br/cceeinterdsm/v/index.jsp?vgnextoid=aedaa5c1de88a010VgnVCM100000aa01a8c0RCRD). O SCDE é o sistema responsável pela coleta diária e o tratamento dos dados de medição, sendo a aquisição destes dados realizada de forma automática, diretamente ao medidor ou através da base de dados do Agente. Este sistema possibilita a realização de inspeções lógicas com acesso direto aos medidores proporcionando maior confiabilidade e precisão dos dados obtidos. Com o SCDE o Agente possui maior praticidade no envio dos dados de medição à CCEE bem como possibilita o acompanhamento diário das informações enviadas. De acordo com o Módulo 12 – "Medição para Faturamento" dos Procedimentos de Rede do ONS [59], os meios de comunicação utilizados para realizar

o "*upload*" dos dados podem ser: VPN, Frame Relay, Internet Banda Larga e, em casos excepcionais devidamente aprovados pelos órgãos competentes, Linha Discada. O Sistema de Medição para Faturamento – SMF garante não só o controle dos processos de contabilização de energia no âmbito da CCEE, como também a apuração das demandas pelo ONS. A Especificação Técnica das Medições para Faturamento, constante no Sub-módulo 12.2 [59], fornece os requisitos técnicos para o SMF, aos quais todos os agentes devem obedecer.

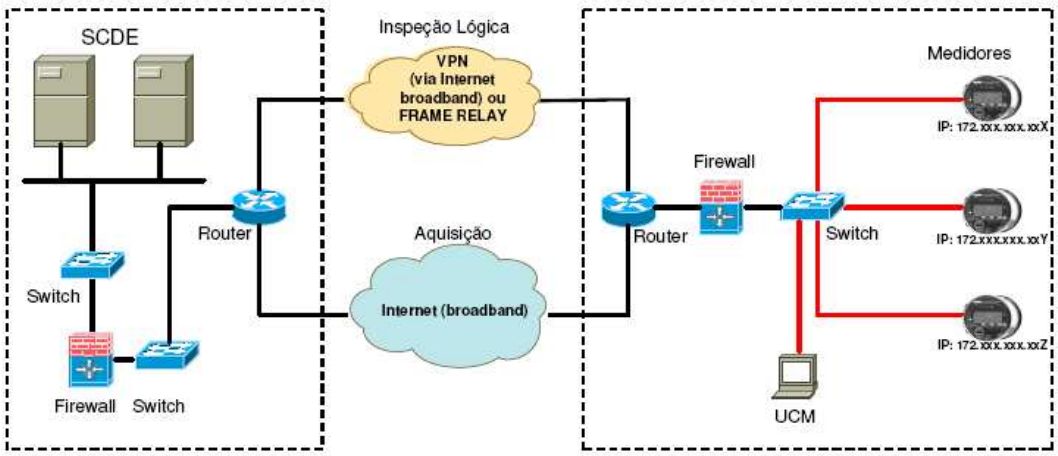


Figura 6.5 - Arquitetura do Sistema de Coletas de Dados de Energia-SCDE (fonte: ONS).

6.2.7 Sistemas de Controle Distribuídos (DCS)

Os sistemas de controle distribuídos são utilizados para operações de controle de processo e/ou aquisição de dados. Em geral, são utilizados como infra-estrutura de comunicação de/para dispositivos de campo, outros sistemas de controle tais como CLPs, UTRs, e mesmo com a rede de dados corporativa para executar aplicações como "*Enterprise Resource Planning*" (ERP). DCS coleta dados de campo e decide o que fazer com eles. Estes dados podem ser também, armazenados para uso futuro, ou para um simples controle de processo em conjunto com dados de outras partes da infra-

estrutura a fim de implementar estratégias de controle mais avançadas, conforme mostrado na Figura 6.6. Embora estes sistemas utilizem tradicionalmente sistemas operacionais proprietários, as novas versões têm optado por sistemas não-proprietários, tais como Windows, Sun Solaris, Linux, etc.. A tecnologia de DCS foi desenvolvida tendo em mente operação eficiente e capacidade de configuração pelo usuário ao invés dos aspectos da segurança e proteção de sistema. Tais tecnologias têm sido desenvolvidas para permitir acesso remoto, via PC, e para visualizar e reconfigurar parâmetros operacionais. As fronteiras práticas e tecnológicas entre DCSs, PLCs e PCs para controle não são tão claras. Sistemas que eram tradicionalmente associados com controle de processo estão sendo usados em aplicações discretas. Do mesmo modo, soluções tradicionalmente discretas estão usadas em controle de processos por lote e contínuo.

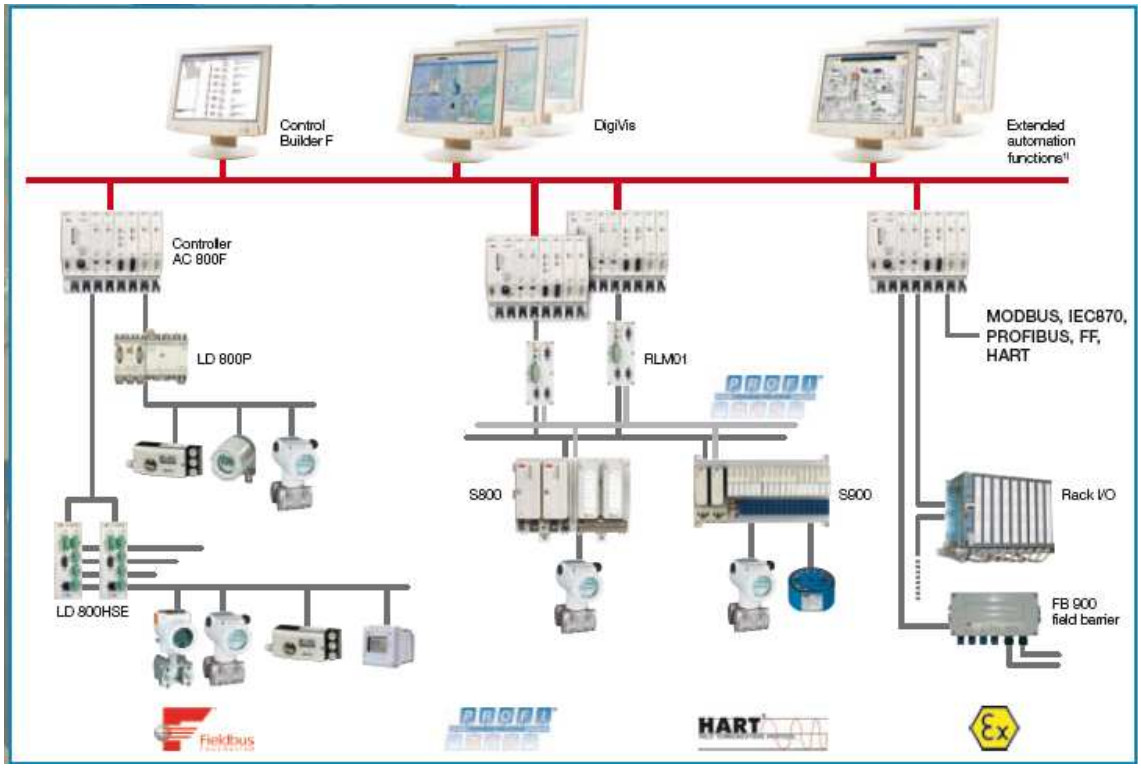


Figura 6.6 - Arquitetura do Freelance 800F Distributed Control System (Fonte: ABB Automation).

6.2.8 Dispositivos de Campo

Sensores de pressão e temperatura, analisadores químicos e atuadores elétricos, são exemplos de dispositivos de campo e compõem a instrumentação do processo, conforme mostrado na Figura 6.6. Dispositivos de campo inteligentes incluem hardware para habilitar a capacidade de calibração em campo, "*upload*" de dados de calibração, etc. Estes dispositivos podem ter enlaces de comunicação em tempo real entre centros de controle, sistemas de gerenciamento da manutenção, PCs, e outros dispositivos dentro e fora da instalação.

6.2.9 Enlaces de Telecomunicações

A operação de sistemas SCADA e EMS é criticamente dependente dos enlaces de telecomunicação que coletam dados de fontes geograficamente dispersas e transmitem instruções de operação e controle para instalações também geograficamente dispersas. No sistema elétrico norte americano [43] estes enlaces de telecomunicações variam de redes privadas a sistemas de multi-redes usando uma combinação de redes privadas e públicas para aquisição de dados e controle. Além dos cabos de comunicação como meio de transmissão são muito comuns os enlaces de comunicações via sistema de microondas ou via satélite principalmente onde a distância e a topografia tornam estes meios um melhor custo-efetivo. A primeira vista, parece que redes privadas sobre controle total dos proprietários seriam uma boa opção para a segurança do sistema. Contudo, mesmo redes privadas estão conectadas a redes externas, tais como, clientes, fornecedores, entidades independentes, etc. Estas conexões podem oferecer uma grande variedade de caminhos e vulnerabilidades para sistemas SCADA e EMS. Sem um

cuidadoso projeto e gerenciamento da segurança, cada um destes enlaces representa um risco em potencial para o sistema como um todo.

Qualquer interligação de telecomunicação que mesmo estando parcialmente fora do controle da empresa responsável pela operação de unidades de geração, transmissão ou distribuição, sejam sistemas SCADA ou EMS, representa um caminho potencialmente inseguro para os negócios da empresa assim como representa uma ameaça ao sistema interligado como um todo. Segundo documento do EPRI [43], durante as preparações para o "bug do milênio", as análises de interdependência identificaram estes enlaces e suas vulnerabilidades no caso de falhas. Este fato passou a ser um excelente ponto de referência para análise de vulnerabilidade cibernética.

No Brasil, o ONS necessita de um sistema de telecomunicações confiável e de qualidade para suportar as atividades de operação e garantir os níveis e padrões de confiabilidade requeridos pelos consumidores e definidos pela ANEEL. O Módulo 13 - "Telecomunicações", dos Procedimentos de Rede [59], define os requisitos dos sistemas de telecomunicações para a Rede de Supervisão do ONS, que se aplicam ao ONS e aos agentes proprietários de instalações/equipamentos pertencentes à Rede de Supervisão. Os serviços de telecomunicações considerados nos Procedimentos de Rede são todos aqueles de telefonia direta, telefonia comutada e de transmissão de dados, entre as instalações dos agentes e as instalações do ONS e que dão suporte para atividades tais como:

- Operação em tempo real;
- Supervisão do sistema de telecomunicações;
- Rede de oscilografia e perturbações;
- Administração da transmissão elétrica;

- Esquemas de controle e segurança;
- Operação dos elos de corrente contínua;
- Normatização, pré-operação e pós-operação; e
- Planejamento e programação da operação.

O Sub-Módulo 2.5 - "Requisitos Mínimos dos Sistemas de Proteção, Supervisão/Controle e de Telecomunicações", dos Procedimentos de Rede [59], classifica os serviços de telecomunicações em 3 grupos distintos:

- Telecomunicação para Teleproteção;
- Telecomunicação para Transmissão de Dados: As funções de supervisão/controle, proteção e registro de perturbações devem utilizar enlaces de telecomunicação distintos e dimensionados de forma a suportar o carregamento imposto pela função. O Sub-Módulo 10.19 – "Requisitos de Telesupervisão para a Operação" dos Procedimentos de Rede [59] deve orientar as interligações de dados entre instalações de transmissão e os centros de operação; e
- Telecomunicação para Transmissão de Voz.

O subitem 3.2 do Sub-Módulo 13.1 – "Telecomunicações – Introdução" dos Procedimentos de Rede [59] especifica que "os agentes deverão prover os serviços de telecomunicações de interesse do ONS, através do seu sistema privado de telecomunicações e/ou através de operadores de telecomunicações, negociando, quando necessário, e acordando entre as partes, a passagem da informação através dos sistemas de telecomunicações de outras empresas de energia elétrica". A Figura 6.7 apresenta as possíveis interligações de comunicação de dados, diretas entre os Centros de Operação

do ONS e as instalações de transmissão e de geração, integrantes da Rede de Operação. As interligações de dados entre os centros do ONS e as diversas instalações da Rede de Supervisão devem ser definidas pelos agentes e apresentadas ao ONS em conformidade com os requisitos especificados no Sub-Módulo 2.5 dos Procedimentos de Rede [59]. Deve-se observar que são exigidos diferentes requisitos para diferentes tipos de recursos de supervisão e controle, o que pode levar a necessidade do uso de interligações com características distintas. Por exemplo, as interligações para atender aos requisitos das funções do sistema SCADA caracterizam-se por:

- Cobrir todas as instalações da Rede de Supervisão;
- Transportar um grande volume de dados com períodos de aquisição que variam de poucos segundos a vários minutos; e
- Conectar instalações, concentradores de dados ou Centros de Operação do Agente aos Centros de Operação do ONS.

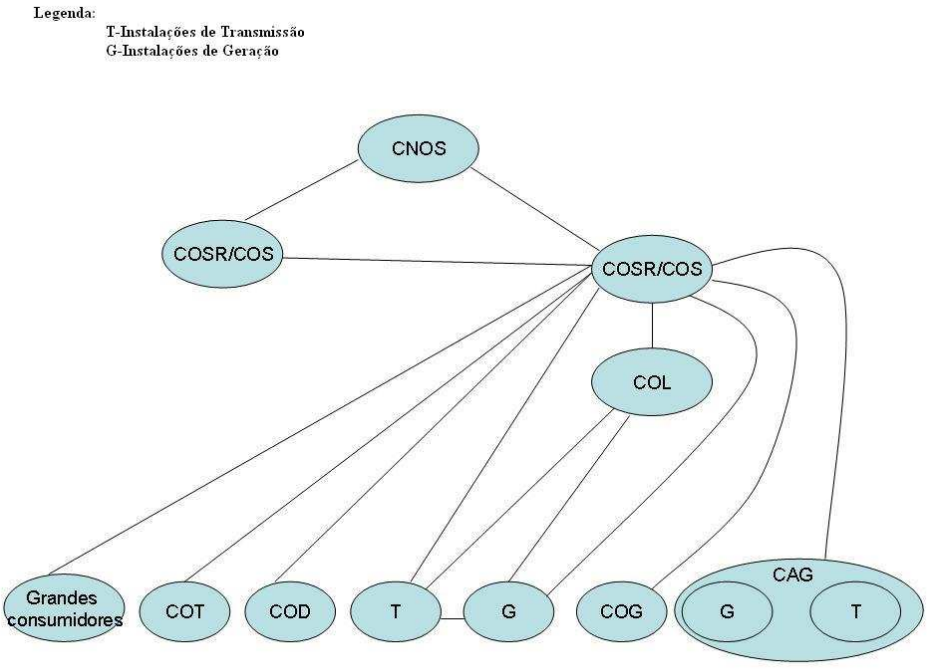


Figura 6.7 - Interligações de comunicação de dados entre COS e Agentes.

Já as interligações para atender aos requisitos do Controle Automático de Geração (CAG) apresentam características como:

- Transporte de dados relativamente pequeno em cada interligação com taxas de transferências de dados relativamente altas e períodos de aquisição tipicamente de 2 segundos; e
- São configuradas com ligação direta entre os centros operação do ONS e aquelas instalações restritas somente ao Controle Automático de Geração (CAG).

6.3 AMEAÇAS E VULNERABILIDADES

Como grandes usuárias dos sistemas de controle e da tecnologia das redes industriais, as empresas do setor elétrico estão sujeitas a ameaças e vulnerabilidades, como ilustra a Figura 6.8 retirada da referência [80].

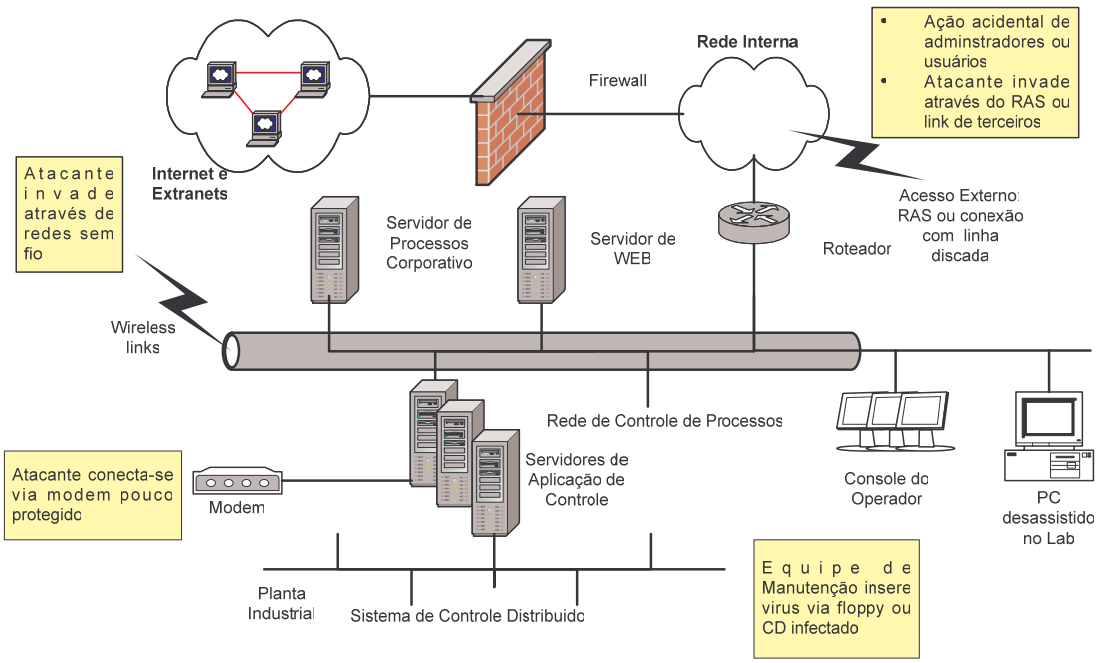


Figura 6.8 - Ameaças e vulnerabilidades presentes em sistemas de controle conectados a Internet ou a Redes proprietárias.

Os possíveis atacantes podem ser divididos em diferentes grupos de pessoas, cada um deles com diferentes características, tais como capacidade, recursos, suporte e motivação. Os principais grupos e suas características são:

- "*Hackers*": São aqueles que possuem recursos computacionais adequados, dedicação e atacam por achar engraçado ou desafiador;
- Empregados: São aqueles que têm conhecimento dos procedimentos internos, têm acesso fácil e atacam com ou sem propósito definido;
- "*Insiders*", empreiteiros e competidores: São aqueles que têm acesso a informações classificadas e possuem conhecimento de operações e de senhas "*default*";
- "*traders*": São aqueles que possuem habilidades computacionais e que poderiam obter ganhos financeiros com as informações obtidas ilegalmente;
- Governos estrangeiros: São aqueles que possuem recursos, tais como conhecimento dos sistemas, computadores, criptógrafos, recursos financeiros, agências de inteligência e interesse em causar prejuízos militares ou econômicos;
- Crime organizado, grupos extremistas e terroristas: São aqueles que possuem a dedicação e o conhecimento dos sistemas computacionais para obter ganhos financeiros e/ou prejudicar grupos que eles se oponham; e
- Alianças de grupos acima citados e com a combinação de motivos.

Desta forma as seguintes ameaças poderiam ser evidentes para uma empresa do setor elétrico:

- Invasão Física: O invasor pode produzir danos não somente a uma parte, mas também a várias partes do sistema, tendo em vista sua natureza integrada/interconectada; e
- Invasão Lógica: Também referenciada como invasão cibernética ou invasão eletrônica, é o tipo de invasão mais difícil de proteger, pois ela não é visível como a invasão física, e possui mais questões a serem consideradas e tratadas.

Uma vez o atacante esteja dentro do sistema de informações do Sistema Elétrico, a referência [123] relata várias ações maliciosas que poderiam ser realizadas, tais como:

- Mudança de valores de dados: Através da manipulação de valores dos dados coletados, o atacante pode enganar os operadores com respeito a valores da potência e das tensões na rede. Se um operador toma decisões baseado em informações corrompidas, ele poderá colocar a rede do sistema elétrico de potência em sérios problemas;
- Mudança de sinais de controle: O atacante poderia bloquear sinais de controle e enviar falsas confirmações. Os operadores poderiam ser levados a pensar que os disjuntores estão fechados quando eles estão abertos, ou que um transformador está apresentando mal funcionamento quando ele não está;
- Abertura de disjuntores: O atacante poderia tomar controle direto da rede e enviar sinais de controle para desligar partes do sistema. As tentativas dos operadores para reinicializar a rede elétrica poderiam ser bloqueadas com o uso de DoS no sistema SCADA; e
- Fraude: Na hipótese da medição da energia elétrica vir a ser feita remotamente, provavelmente através de redes IP, os atacantes poderiam manipular fraudulentamente estas medidas.

Os sistemas de informação de uma organização são mais vulneráveis no ponto em que a conectividade é maior e o controle de acesso é mais fraco. Se um invasor optasse por atacar a rede do sistema elétrico eletronicamente, ao invés de fisicamente, as opções a considerar seriam: os centros de controle, as subestações e a infra-estrutura de comunicações [53].

A referência [78] aponta as vulnerabilidades mais comuns encontradas em sistemas SCADA e em redes corporativas que impactam a relativa segurança dos sistemas SCADA. Dentre eles, destaca-se a disponibilidade de informações acerca das empresas encontradas nos websites, o uso de arquiteturas de redes de comunicação de dados inseguras e a falta de monitoramento/gerenciamento destas redes em tempo real.

Os itens a seguir descrevem a natureza das vulnerabilidades de cada setor, tendências e o modo de ataque.

6.3.1 Vulnerabilidades no Centro de Controle

Não existe configuração padrão para um centro de controle (vide Figura 6.1). Os sistemas variam de "mainframes" desenvolvidos a mais de 20 anos por especialistas da própria organização, até sistemas cliente-servidor em rede baseados em sistema operacional Unix ou Windows e desenvolvidos comercialmente por empresas contratadas. A tendência da indústria é procurar um sistema "padrão", baseado em tecnologia distribuída cliente-servidor, a fim de reduzir o risco e minimizar os custos de projeto.

Observando o diagrama da figura 6.8, mostrada anteriormente, nota-se que um invasor pode ter acesso ao centro de controle através de várias interfaces, a saber:

- Conexões ao Sistema de Informação Corporativo: Embora não seja uma prática comum, esta é uma forte tendência nos dias de hoje, pois muitas empresas consideram o risco como sendo válido pelo valor das informações acessadas dos centros de controle. Soluções comuns para este tipo de conexão incluem o uso de firewall ou de esquemas de roteamento usando sub-redes para criar uma conexão segura entre o sistema de informação corporativo e o EMS. Contudo, esta tendência aumenta o risco de ataques. Apesar das salvaguardas utilizadas para isolar os centros de controle, eles ainda continuam vulneráveis.
- Conexões com outras empresas do setor: Muitas empresas do setor elétrico possuem conexões entre seu centro de controle e o centro de controle de outras empresas ou o centro de controle regional. Muitos destes enlaces de comunicação são num único sentido, e transportam dados dos sistemas que os operadores utilizam para balancear a carga, escalonar a transmissão, calcular o despacho econômico e realizar análises de segurança. Controles ao nível de aplicação e protocolos proprietários tornam mais difíceis estes enlaces para um ataque eletrônico. Caso estas empresas sigam as novas tendências de utilização de protocolos padrões para interconexão de redes, o risco de ataques irá aumentar sensivelmente. A desregulamentação do setor é outro fator que pode vir a ocasionar o aumento da vulnerabilidade das conexões entre as novas empresas formadas.
- Suporte para desenvolvimento e manutenção fora da empresa ("*outsourcing*"): Esta é uma tendência que vem ocorrendo com a maioria das empresas do setor elétrico e que utilizam outras empresas para realizar a "*customização*",

manutenção e suporte de sistemas EMS. Para atender a esta nova tendência as empresas do setor elétrico estão fornecendo acesso remoto a fabricantes e integradores de sistemas. Este acesso remoto em geral é realizado através de modems discados, embora existam conexões dedicadas para este fim. Estas interconexões representam uma vulnerabilidade em potencial à segurança do sistema. Na literatura encontramos várias destas ocorrências, como o caso relatado em [48], ocorrido em Janeiro de 2003, onde o laptop do empregado de uma empresa prestadora de serviços foi conectado a rede de uma usina nuclear via modem e infectou o sistema de monitoramento de segurança da usina nuclear em Davis-Besse, EUA, com o "*worm*" Slammer. Outro exemplo, neste mesmo sentido, é citado em [53].

- Administração e Manutenção Remota: Muitas empresas do setor elétrico têm permitido que equipes do sistema de informação e da operação acessem sistemas remotamente após horário normal de funcionamento. Este acesso remoto é realizado através de modems discados na rede do EMS. Estas equipes podem discar para os pontos de acesso disponíveis na rede do EMS e realizar operações de "*troubleshooting"* e administração de sistemas, e, em alguns casos, operar aplicações do EMS. Estes enlaces de modems discados representam pontos de acesso para invasores eletrônicos. Muitas empresas têm usado medidas, como sistemas de autenticação, para reforçar o controle de acesso a estes pontos.
- Impactos: A despeito do local onde está o ponto de acesso, uma vez dentro do sistema de controle o invasor poderá "derrubar" o EMS. Um invasor com bons conhecimentos do sistema elétrico pode empregar opções bem sutis, como corromper as bases de dados, produzindo graves efeitos econômicos na concessionária, por alterar as operações de faturamento. Outra forma seria enviar

falsos comandos para o sistema para abrir e fechar relés, desligar linhas e afetar a geração. Mais grave ainda seria manipular o fluxo de dados para o centro de controle, fazendo com que os operadores respondessem a indicações espúrias. Felizmente o número de pessoas com conhecimento suficiente para atacar o sistema desta forma é reduzido.

6.3.2 Vulnerabilidades em Subestações

Subestação é um local, onde existe um conjunto de componentes elétricos, utilizados para dirigir e controlar o fluxo de energia do sistema elétrico, procurando garantir, de forma contínua e segura, o transporte desse fluxo, vinculando as suas fontes de produção e de transmissão aos mais diversificados centros de consumo.

De forma a garantir a máxima segurança de operação e o serviço a todas as partes componentes dos sistemas elétricos, as subestações são providas de equipamentos de manobra para a distribuição da energia elétrica através de circuitos e de equipamentos de proteção para garantir a segurança do sistema em condições de defeito.

Num esforço de melhorar a qualidade do serviço prestado aos seus clientes com o menor número possível de pessoal, as empresas do setor elétrico vêm automatizando as operações de subestações com unidades de terminais remotas e uma variedade de dispositivos eletrônicos inteligentes, como aqueles especificados anteriormente no item 6.2, passando a utilizá-los no local dos dispositivos fixos e manuais. Contudo, tanto as UTRs quanto os novos dispositivos automáticos são susceptíveis aos ataques

eletrônicos. A Figura 6.9, retirada da referência [75], apresenta alguns pontos de vulnerabilidade para uma invasão eletrônica em uma subestação.

- Dispositivos Digitais Programáveis: Discando para a porta de status do disjuntor conectada a um dispositivo programável, o engenheiro pode fazer o "*reset*" do dispositivo ou mesmo selecionar um dos seus níveis de proteção. Um invasor que identifica a linha telefônica servindo tal dispositivo poderia discar para uma porta não protegida e realizar o "*reset*" do dispositivo para um nível maior de tolerância. Ao realizar isto, ele poderia estar destruindo fisicamente algum equipamento da subestação. Outra ação maliciosa seria tornar o dispositivo mais sensível que a condição normal e fazer com que o sistema se desligue por auto-proteção. Muitas empresas não possuem qualquer tipo de segurança ou controle de acesso para dispositivos possuindo "*dial-in access*" [53].

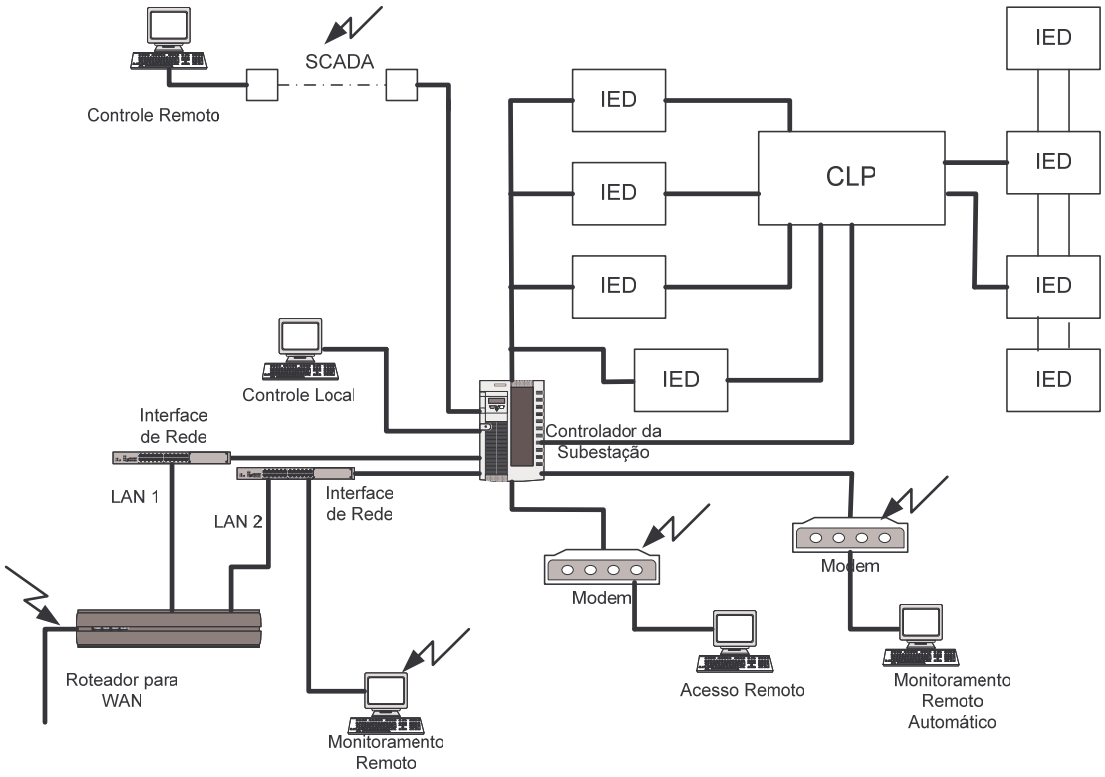


Figura 6.9 - Pontos de Vulnerabilidades sujeitos a invasão eletrônica [75].

- Unidade de Terminal Remota: Além de coletar dados, uma UTR funciona também como unidade de troca de sinais de controle para equipamentos de transmissão e distribuição. Várias empresas do setor elétrico relataram que possuem portas de manutenção em UTRs, acessíveis remotamente através de modem discado [53]. Um invasor poderia discar para esta porta e enviar sinais de comando para equipamentos da subestação ou mesmo corromper dados enviados ao centro de controle. Devido a natureza do sistema elétrico interligado, "invadir" uma UTR com intuitos maliciosos pode significar um efeito de desligamento em cascata para o sistema como um todo.

Oman et al [75] elaborou uma matriz de vulnerabilidades de equipamentos presentes em uma subestação. Esta matriz aponta as vulnerabilidades e os riscos associados a estas vulnerabilidades para cada equipamento listado, bem como as técnicas para mitigar tais riscos.

A referência [81] investiga as ameaças de ataques em redes de comunicação dados localizadas em subestações. Os autores listam 3 tipos fundamentais de ataques e propõe um protocolo de comunicação seguro para conter estes ataques e reduzi-los a um modo de falha que pode ser tratado de forma similar a outras falhas não maliciosas pelos mecanismos de proteção.

6.3.3 Vulnerabilidades nas Comunicações

A Figura 6.2, apresentada anteriormente, representa uma típica Infra-estrutura de comunicação de dados para o sistema elétrico. As empresas do setor utilizam um conjunto de meios de comunicação proprietário e público, variando de radio microondas

e fibra ótica a redes públicas de comunicação de dados. Qualquer desses meios pode vir a ser explorado para um ataque cibernético. Um ataque nesta infra-estrutura de comunicações em conjunto com um ataque ao sistema elétrico de potência constitui o que as empresas do setor chamam de "um cenário de pesadelo" [53]. Restaurar o sistema interligado seria extremamente difícil e perigoso se todos os meios de coordenação entre os centros de controle e os elementos de transmissão estivessem fora de serviço. Para o Sistema Interligado Nacional - SIN, o Módulo 13 dos Procedimentos de Operação [59] especifica os Requisitos dos Sistemas de Telecomunicações para a Rede de Supervisão do ONS. Este módulo especifica que os agentes podem usar enlaces de comunicação de propriedade da empresa de energia elétrica (Infra-estrutura Privada) ou das concessionárias de serviços de transmissão de dados (Infra-estrutura Pública). As vulnerabilidades apontadas para cada modelo são:

- Vulnerabilidades na Infra-estrutura Privada: A maioria das redes de comunicação privada do setor elétrico é composta por sistemas de microondas e de fibra ótica. Estas instalações são consideradas de suma importância para as empresas do setor. Em muitos casos, as empresas vendem o excesso da capacidade destas redes para empresas de transmissão de dados comerciais, ou mesmo planejam usar esta infra-estrutura para entrar no mercado de comunicação de dados. A despeito das empresas do setor de dizer o contrário, a infra-estrutura de comunicações privada da empresa concessionária é tão vulnerável quanto às redes públicas. Segundo [53], já foram relatados roubos no serviço de voz, bem como perda dos serviços de voz e de dados resultantes de danos físicos.
- Vulnerabilidades na Infra-estrutura Pública: Segundo [53], nos EUA aproximadamente um terço do tráfego das comunicações de controle das

empresas de energia elétrica é feito através das redes públicas. Muitas empresas utilizam redes públicas para aumentar a capacidade de suas redes privadas e formar canais de comunicação redundantes entre as subestações mais importantes e aquelas localizadas em regiões geograficamente remotas. Estas empresas estão cientes das ameaças que as redes públicas oferecem e por isso mesmo tomam medidas para mitigar o risco nas conexões consideradas mais críticas, tais como, usar meios de transmissão redundantes, requerer o roteamento diferente para as linhas alugadas contratadas, usar VPN, etc.

A referência [82] aponta as grandes deficiências nos atuais sistemas de comunicações e de informação em empresas do setor elétrico dos EUA e propõe uma nova arquitetura. Esta constatação foi feita após a análise de 162 distúrbios de 1979 a 1995 relatadas pelo NERC. A arquitetura proposta inclui os sistemas de controle e automação em todos os níveis, de subestações ao Centro de Operações do Operador do Sistema, levando em conta os requisitos de dados em tempo real, segurança, disponibilidade, escalabilidade e qualidade de serviço (QoS) adequada. Este modelo utiliza múltiplos canais de comunicação empregando uma grande variedade de tecnologias para transmitir dados e sinais de controle em tempo real.

6.4 MELHORES PRÁTICAS PARA PROTEÇÃO DE SISTEMAS DE CONTROLE

As empresas de energia elétrica utilizam uma série de mecanismos para proteger a rede elétrica de interrupções. Entretanto, muitos destes mecanismos somente são funcionais se não há interrupção do fornecimento de dados do campo, pois se o fluxo de

informações é cortado os resultados serão irreais. Outro ponto é que estes mesmos mecanismos não consideram elementos externos ao sistema elétrico.

Além monitorar ativamente o status do sistema elétrico, muitas empresas tem adotado medidas para proteger seus centros de controle e EMS de ataques físicos e de falhas do sistema. Uma das medidas é manter centros de controle de "*back-up*". Outra medida é ter as instalações de comunicações completamente redundantes e com seu próprio centro de controle. Em muitos casos as empresas possuem "*dial-back modem*" e "*firewalls*" para as interfaces do EMS com o mundo externo. Muitos sistemas suportam, também, "*logins*" e "*passwords*" individuais, além de alarmes e "*logs*" de eventos.

Em geral a segurança física é mais considerada que a segurança cibernética nas empresas do setor elétrico. Outro ponto é que muitas dessas empresas possuem equipes para tratar a segurança dos sistemas corporativos além de equipes para realização de auditorias internas. Contudo estas facilidades raramente se voltam para a área operacional da empresa, como os sistemas de controle. Tomando em consideração as reflexões encontradas em [62] e as pesquisas realizadas junto a diversas empresas, apresentadas em [53], e os passos listados em [77], sugerem-se algumas medidas básicas para melhorar a segurança, tais como:

- Estabelecer Políticas de Segurança da Informação;
- Conduzir avaliações e auditorias sobre segurança;
- Conduzir estudos de análise de risco e vulnerabilidades;
- Garantir o controle do acesso quando usando conexões discadas;
- Utilizar as opções de segurança existentes;
- Eliminar falhas de segurança existentes;

- Avaliar novas tecnologias de segurança;
- Empregar novas tecnologias de segurança com uma melhor relação custo-efetividade;
- Melhorar a coordenação entre as equipes de operação e de segurança de informação corporativa;
- Aprimorar a capacidade técnica da equipe de segurança; e
- Estabelecer programas de conscientização sobre segurança dentro da organização.

Em termos de mecanismos e ferramentas, muitos elementos existem para defender os sistemas. Dentre as ferramentas mais comuns citamos "*passwords"*, "*firewall*", sistemas de detecção de intrusão (IDS), "*Virtual Private Network (VPN)"* e controle de acesso, dentre outros. A descrição destes mecanismos e de outros é amplamente encontrada na literatura: [23, 24, 34, 43, 47, 53, 61, 64, 65, 66, 67, 68].

6.5 ANÁLISE DE VULNERABILIDADES

Recentemente o mundo das tecnologias da informação tem visto um crescimento exponencial no número de vulnerabilidades relatadas para os sistemas de informação em rede. A Página do "CERT-CC Statistics 1988-2006" (http://www.cert.org/stats/) relata que as vulnerabilidades cibernéticas cresceram de menos de 300 por ano em 1998 para cerca de 8000 casos relatados em 2006. Este crescimento sem precedentes tornou-se um dos principais desafios enfrentados pelas equipes de segurança operacional que devem não somente considerar o número de ataques, mas também como estes ataques podem ser combinados sob várias formas. Fica evidente a necessidade de uma

metodologia para organizar as possibilidades de ataque, compreender suas inter-relações e ordená-las segundo o risco.

Tem-se criado vários modelos para classificar as vulnerabilidades. Muitos destes modelos são taxonomias, isto é, um sistema de classificação que permite que as vulnerabilidades sejam unicamente identificadas. McHugh, em [83], relata as primeiras tentativas de criar-se uma taxonomia para classificar vulnerabilidades. A compreensão das vulnerabilidades é um passo crítico para a compreensão das ameaças que elas representam. O uso correto da metodologia para classificar vulnerabilidades possibilita a coleta da freqüência de dados, análise de tendências, correlação de incidentes, "*exploits*" e artefatos, bem como a avaliação da efetividade das contramedidas. Segundo [84], existem esquemas de classificação que se baseiam em relatórios de vulnerabilidades e não numa correta análise do domínio do problema. Os autores desta referência propõe um esquema de classificação que usa pares de atributo-valor para fornecer uma visão multidimensional das vulnerabilidades. Atributos e valores são selecionados baseados numa classificação que permite que as vulnerabilidades sejam exploradas por uma dada técnica ou que se determine as contramedidas efetivas.

As ferramentas para avaliação de vulnerabilidades determinam quando um computador ou rede é vulnerável para ataques conhecidos. Elas podem ser passivas ou ativas. As primeiras realizam uma varredura ("*scan*") do computador no qual ele reside em busca de configurações inseguras, versões de software que contém falhas que podem ser exploradas ("*exploitable flaws*") e senhas fracas. Ferramentas ativas residem num único computador e realiza a varredura da rede procurando por vulnerabilidades. A ferramenta envia uma série de pacotes na rede para determinados computadores e a

partir das respostas obtidas a ferramenta pode determinar os serviços e o sistema operacional de cada computador. Além disso, ele pode identificar versões específicas de software e determinar a presença ou ausência de "*patches*". Ela compara a informação coletada com uma biblioteca de número de versões de software, sabidamente inseguros, e determina se os computadores daquela rede são vulneráveis a ataques conhecidos. Exemplos deste tipo de ferramenta são, dentre outros:

- "*AVAST - Automated Vulnerability Analysis Support Tool*" (http://www.jhuapl.edu/ott/technologies/technology/articles/P02124.asp)
- "*GFiLANguard Network Security Scanner*" (http://www.gfi.com/lannetscan/?adv=69&loc=318&adclickid=11845184)
- "*HAVAT – Host Audit Vulnerability Analysis Tool*", (http://sourceforge.net/projects/havat/);

Dentre as pesquisas realizadas na direção da modelagem de ataques e vulnerabilidades podemos citar a técnica de "*Attack Trees*", inicialmente descrita por Schneier [85] e usada por Byres et al em [86] a fim de avaliar as vulnerabilidades em sistemas SCADA. Esta técnica permite um modo estruturado e flexível para conduzir análise de segurança em protocolos, aplicações e redes. Também Moore et al [87] desenvolveu uma aplicação mais formal da técnica introduzindo notação padronizada e fornecendo exemplos mais complexos. [88] desenvolveu a interpretação formal para compreender mais precisamente como "*attack tree*" pode ser manipulada durante as fases de construção e análise.

A referência [129] apresenta um modelo desenvolvido para sistemas EMS e SCADA que permite calcular a vulnerabilidade do dispositivo e ajudar os operadores e

administradores de subestações a identificar e "endurecer" ("*hardening*") as porções do sistema de controle que são mais vulneráveis a ataques cibernéticos. Os autores utilizam teoria de grafos para modelar os dispositivos de controle e proteção do sistema elétrico e sua conectividade associada. É introduzido o conceito de "caminho de visibilidade do dispositivo" e utiliza-se uma aplicação Prolog para calcular o "nível de vulnerabilidade do dispositivo" para um dispositivo alvo em uma subestação hipotética.

CAPITULO 7

DEFENDENDO SISTEMAS DE INFORMAÇÃO ATRAVÉS DA DETECÇÃO DE INVASÕES

Ataques em sistemas computacionais e redes de computadores têm aumentado significantemente nos últimos tempos. A ocorrência de ataques na forma de vírus, DoS, DDoS, worms, etc., têm sido relatados em várias plataformas. Sistemas de Detecção de Intrusão ("*Intrusion Detection Systems – IDS*") são um importante componente nos mecanismos de "*defense-in-depth*" em sistemas computacionais e redes de computadores e tem sido amplamente discutido desde o inicio dos anos 80. Nos anos 90 detecção de intrusão tornou-se um "*hot topic*" e começaram a aparecer aplicações comerciais com esta finalidade. Também existem vários protótipos resultantes de pesquisas, dos quais alguns evoluíram em produtos comerciais. Um dos mais utilizados é o SNORT, software de código aberto e distribuído do site: http://www.snort.org/. Em [90] e [91] podemos encontrar um ótimo "*survey*" deste tópico com uma extensa bibliografia. Também em [116] e[118] encontramos uma extensa bibliografia sobre o assunto. Um bom livro texto sobre o assunto pode ser encontrado em [132]. Em [120] encontramos uma lista de produtos de IDS comerciais, de domínio público e de pesquisa. O documento do NIST [92] "*Intrusion Detection Systems*" apresenta um excelente estudo sobre IDS bem como considerações técnicas para seleção e implementação de IDSs. Uma evolução dos IDS é apresentada em [93]. Neste documento é introduzido o IDPS: "*Intrusion Detection and Prevention Systems*". Estes sistemas além de detectar a intrusão, possuem a capacidade de tentar parar o possível

incidente. IDPS está bem descrito no "*NIST Special Publication 800-94 – Guide to Intrusion Detection and Prevention Systems*", acessível do site http://www.nist.gov . Neste capitulo iremos comentar sobre as ferramentas de detecção de ataques ou invasões e as recentes pesquisas no desenvolvimento destas ferramentas.

7.1 DETECÇÃO DE INTRUSÃO

A detecção de intrusão é o processo de detectar o uso não autorizado (ataque ou invasão) a um computador ou a uma rede de computadores. Sistemas de detecção de intrusão, ou IDS, são sistemas de hardware ou software que detectam este abuso, detectando, assim, as tentativas de comprometer a confidencialidade, a integridade e a disponibilidade de um computador ou de uma rede de computadores. As fontes de ataque podem ser a Internet, usuários autorizados que abusam dos privilégios dado a eles, e usuários não autorizados, que tentam ganhar privilégios não autorizados.

A Figura 7.1 apresenta os componentes de um IDS genérico baseado no modelo estudado por [90]. A figura mostra as três fases de um IDS genérico:

- Coleta de Dados;
- Detecção; e
- Resposta.

Segue uma breve descrição de cada componente:

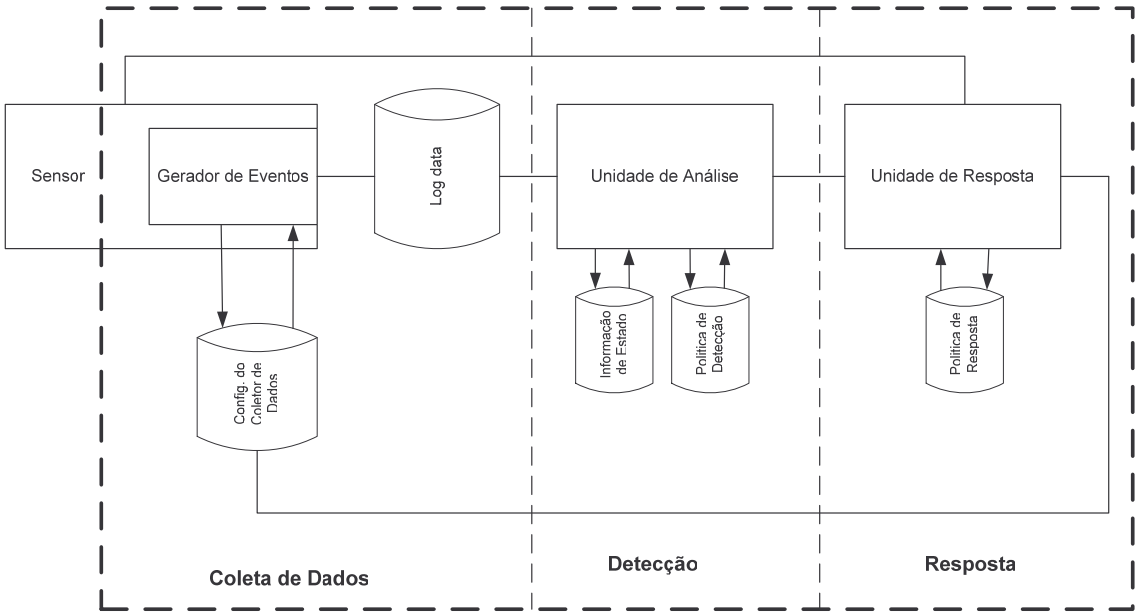


Figura 7.1 - Componentes de um IDS .

- Sensor: É o subsistema que possui os mecanismos para coletar os vários tipos de dados, tal como, o tráfego da rede, os logs do sistema operacional e os logs de aplicativos.
- Gerador de Eventos: Cuida da informação registrada.
- Log Data: Depósito para os dados antes de serem enviados para a Unidade de Análise. Estas informações podem ser usadas para a investigação de alarmes e análise forense.
- Unidade de Análise: Implementa o algoritmo de detecção. O método mais simples é o uso de "*scripts*" para encontrar textos que identificam o tipo de invasão. Outras formas incluem análise de assinaturas e detecção de anomalias;
- Política de Detecção: Contém as informações pré-programadas de como detectar as intrusões. Depende do tipo de técnica empregada pela Unidade de Análise.

- Informação de Estado: É a base de dados que contém as informações dinâmicas usadas para detecção. Depende do tipo de técnica empregada pela Unidade de Análise.
- Unidade de Resposta: Recebe as informações classificadas pela Unidade de Análise como invasiva ou anômala, dependendo do algoritmo usado.
- Política de Resposta: É a base de dados que contém as regras pré-programadas que decidem como responder a diferentes eventos.

O uso de detecção de intrusão está se tornando uma necessidade na infra-estrutura de segurança de qualquer organização. Porém a questão para os profissionais de segurança não é a utilização destes sistemas, mas sim, que características e capacidades devem ser incorporadas nestes sistemas. Podemos dizer que existem 3 razões principais para se usar um IDS [94]:

- Detectar ataques e outras violações de segurança;
- Proibir atacantes de vasculhar a rede ("*scanning*");
- Documentar a ameaça de invasão em uma organização.

Existem vários tipos de IDS disponíveis hoje em dia, caracterizado por diferentes formas de monitoramento e de análise. Cada um tem um uso distinto, vantagens e desvantagens.

A Figura 7.2, apresentada em [120], ilustra uma pequena empresa configurada com firewalls e detectores de intrusão. Computadores configurados como sensores de rede extraem pacotes suspeitos dos três principais segmentos da rede e os enviam para a

estação de análise específica da rede. O Servidor de Web e as estações de trabalho executam software para monitorar interações suspeitas com o sistema operacional, relatando-os para a estação de análise específica do host. Além disso, o servidor de web procura por abusos tais como "*CGI-bin exploits*" que são específicos em servidores de HTTP. Os analisadores reportam a uma console de gerenciamento que serve como interface para o usuário do IDS. Outras formas mais elaboradas são possíveis. Por exemplo, um analisador poderia usar as entradas de um ou de todos os sensores para decidir se um ataque está acontecendo.

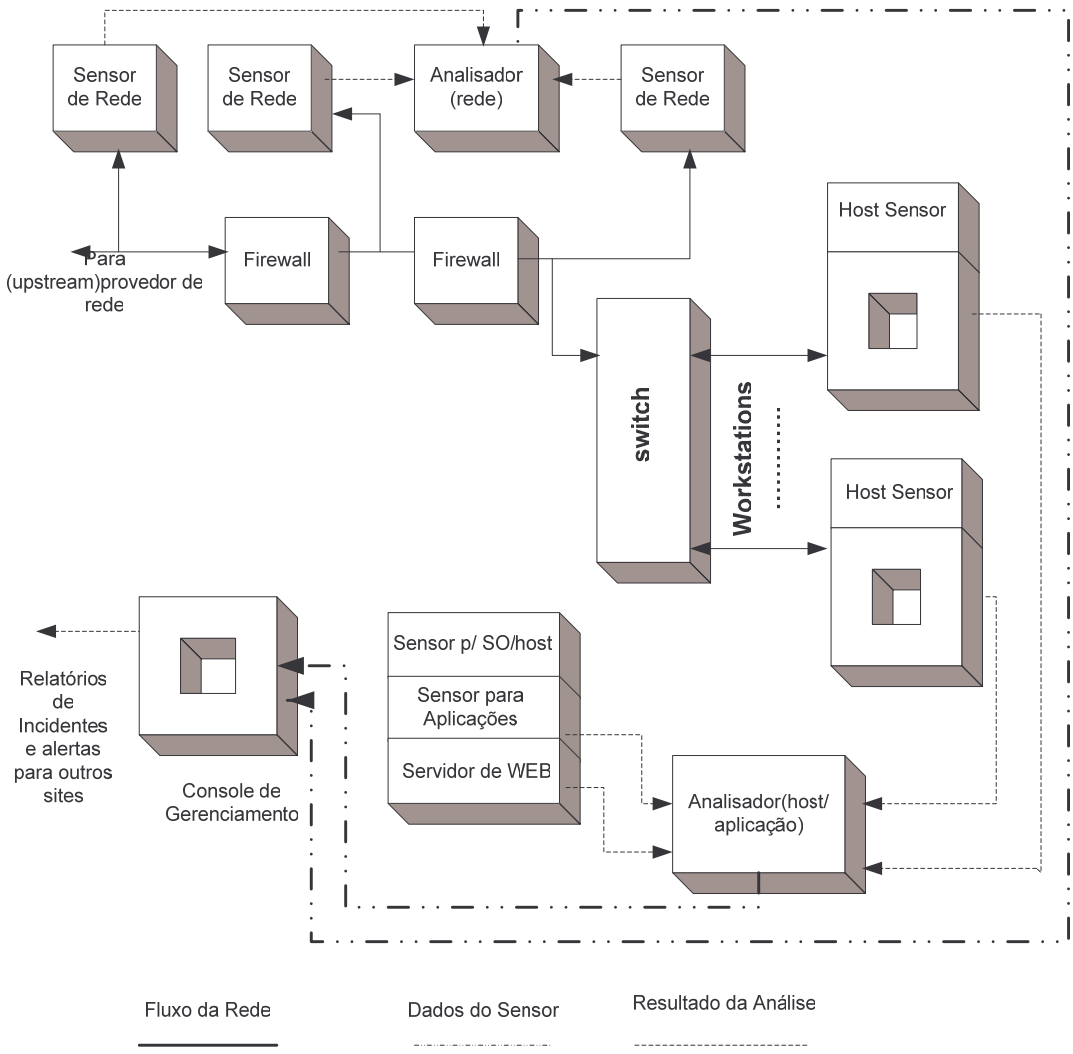


Figura 7.2 - Estrutura de um sistema utilizando IDS.

7.1.1 Modelos de Monitoramento

Um modo de classificar um IDS é verificar o que ele monitora. Alguns IDSs "escutam" o "*backbone*" da rede e analisam os pacotes para determinar os atacantes. Outros IDSs residem no computador que eles defendem e monitoram as atividades do sistema operacional buscando sinais de intrusão. Ainda existem outros que monitoram aplicações individuais [95].

a) IDS baseado em Rede

IDS baseado em rede, o modelo mais comercializado atualmente, detecta ataques capturando e analisando pacotes da rede. "Escutando" o "*backbone*", este tipo de IDS pode monitorar uma grande quantidade de informação através da captura do tráfego da rede ("*sniffing*") realizado por um conjunto de computadores localizados em vários pontos distintos da rede. Estes computadores reportam para o console de gerenciamento do processo. Desde que nenhuma outra aplicação seja executada nos computadores utilizados por este tipo de IDS, eles estão seguros contra ataques. Muitos deles possuem modo "*stealth*", o que o torna extremamente difícil para um atacante localizar sua presença. Este tipo de IDS tem pouco impacto na rede existente, porque eles são dispositivos passivos, que "escutam" a rede sem interferir com a operação normal da rede.

b) IDS baseado em Host

IDS baseado em "*host*" opera analisando a atividade em um determinado computador. Dessa forma ele deve coletar informação do "*host*" que ele está monitorando. Isto permite que o IDS analise atividades no "*host*" numa granularidade muita fina e determinar exatamente quais processos e usuários estão realizando

atividades maliciosas no sistema operacional. Alguns IDSs simplificam o gerenciamento de um conjunto de hosts mantendo as funções de gerenciamento e relatório de ataques centralizado em uma única console de segurança. Outros geram mensagens que são compatíveis com o sistema de gerenciamento da rede. Neste caso este tipo de IDS pode detectar ataques que não são detectáveis pelos IDSs baseados em rede, pois eles possuem uma visão local a um determinado "*host*". Entretanto o IDS baseado em host pode ser atacado e desabilitado por um atacante mais experiente, pois parte deste sistema reside no host que está sendo atacado. Outra desvantagem é que este tipo de IDS tem dificuldade de detectar e operar em face a um ataque de DoS, pois neste caso ele irá exaurir os recursos do computador que está sendo monitorado.

c) IDS baseado em Aplicações

Este tipo de IDS monitora os eventos resultantes da execução da aplicação. Em geral ele detecta ataques analisando os arquivos de log da aplicação. Através da interface direta com a aplicação e tendo significante domínio ou conhecimento da aplicação, IDS baseado em aplicação tem maior probabilidade de discernir atividades suspeitas na aplicação, permitindo aos administradores seguir atividade não autorizada de usuários individuais. A desvantagem deste modelo é que eles são mais vulneráveis que os outros 2 modelos, podendo ser atacado e desabilitado, pois eles executam como uma aplicação no host em que estão monitorando.

7.1.2 Modelos para Análise de Eventos

Como vimos no item 7.1, existem 2 modelos para a análise de eventos: análise de assinatura e detecção de anomalia [96]. Análise de assinatura é a técnica utilizada pela maioria dos sistemas comerciais. Neste caso, padrões conhecidos de invasão

(assinaturas de invasão) são utilizados para tentar identificar as invasões quando elas ocorrem. No outro modelo, denominado detecção de intrusão por anomalia, é assumida que a natureza da invasão é desconhecida, mas que a invasão resultará em um comportamento diferente daquele normalmente visto pelo sistema. A detecção de anomalia ainda é assunto de muita pesquisa e é usado de forma limitada por alguns IDSs. Muitos sistemas de detecção combinam ambos modelos, sendo um bom exemplo disso o sistema IDES [97].

a) IDS baseado em Assinaturas

A detecção baseada em assinaturas, ou detecção de abuso, procura por atividades que casam com um conjunto predefinido de eventos o qual descreve um certo ataque conhecido. Desta forma este modelo de detecção deve ser especificamente programado para detectar cada ataque conhecido. Esta técnica é extremamente efetiva, sendo o principal método utilizado em produtos comerciais para detectar ataques. A principal vantagem desta técnica é que ela é capaz de detectar ataques sem um número muito alto de alarmes falsos. Por outro lado, eles devem ser programados para detectar cada tipo de ataque e, portanto devem ser constantemente atualizados com assinaturas para novos ataques. Exemplos de técnicas de detecção de abusos podem ser encontradas em IDIOT [98], STAT[99] e SNORT[100].

b) IDS baseado em Anomalias

IDS baseado em anomalias determina ataques identificando o comportamento não usual (anomalias) em um computador ou na rede. Seu funcionamento é baseado na

observação de que os atacantes comportam-se de maneira diferente do usuário normal e, portanto, podem ser detectados por sistemas que identificam estas diferenças. Este modelo estabelece uma linha de operação básica de comportamento normal criando um "perfil" para certos usuários ou conexões de rede, e, então, medindo estatisticamente quando uma atividade monitorada se desvia da Norma. Estes perfis são criados a partir de dados históricos coletados por certo período de operação normal do sistema. Infelizmente, estes IDSs produzem um grande número de alarmes falsos, pois o comportamento normal do usuário e da rede pode variar brutalmente. Esta natureza imprevisível dos usuários e do tráfego das redes requer muitos treinamentos de conjuntos de "logs" do sistema a fim de caracterizar os padrões de comportamento normal. Os detectores coletam os eventos e usam uma variedade de outras medidas para determinar quando a atividade monitorada desvia-se da normalidade. [101] descreve as medidas e técnicas usadas neste modelo:

- Detecção por limites de operação: Neste caso certos atributos do usuário ou do sistema são expressos em termos de contadores, com um certo nível de folga permitido. Tais atributos são especificados como números de arquivos acessados por um usuário num dado período de tempo, o número de tentativas que falharam para fazer o "*login*" no sistema, a quantidade de CPU utilizada por um processo, etc. Este nível pode ser estático ou heurístico (isto é, projetado para alterar a partir dos valores observados ao longo do tempo);
- Medidas Estatísticas: Pode ser paramétrico, onde se assume que a distribuição de certos atributos definidos no perfil ajusta-se a um certo padrão, ou não paramétrico, onde a distribuição dos atributos obtidos por perfil são "aprendidos" de um conjunto de valores históricos, observados ao longo do tempo.

- Medidas baseadas em regras: Similar ao modelo não paramétrico anterior, na qual os dados observados definem padrões aceitáveis de uso, mas com a diferença de que estes padrões são especificados por regras ao invés de valores numéricos.
- Outros modelos incluindo redes neurais, algoritmos genéticos e modelos de sistemas imunológicos.

A despeito do grande número de alarmes falsos produzidos, pesquisadores afirmam que IDSs baseados em anomalias são capazes de detectar ataques nunca vistos anteriormente, diferentemente dos IDSs baseados em assinaturas que se baseiam na análise de ataques passados. Exemplos de sistemas IDS com detecção de anomalias são o IDES [97] e EMERALD [102].

7.1.3 Taxonomia dos Princípios de Detecção de Intrusão

A Tabela 7.1 apresenta a taxonomia descrita por [91]. Como já comentado o processo de detecção de intrusão é dividido em dois grandes grupos: por anomalia e por assinatura ou abuso. A detecção por anomalia divide-se em 2 grandes grupos:

- Auto-aprendizagem: É feita através de exemplos sobre o que é considerado normal para a instalação. Em geral isto é realizado através da observação do tráfego por um longo período de tempo.
- Programado: Neste caso é necessário que alguém, usuário ou especialista, ensine o sistema – ou seja, programe-o – para detectar certos eventos anômalos. Desta forma o especialista indicará o que será considerado anormal o suficiente para

que o sistema identifique como uma violação de segurança. Entre os exemplos podemos citar aqueles baseados em regras e a modelagem por séries temporais.

A detecção por assinatura é programada com regras explicitas usando modelagem de estado, sistemas especialistas ou sistemas baseados em regras.

Tabela 7.1 - Classificação dos princípios de detecção segundo.

Anomalia	**Auto-aprendizagem**	Sem uso de séries temporais	Modelagem usando regras
			Estatística descritiva
		Séries temporais	ANN
	Programado	Estatística descritiva	Estatístico
			Baseado em regras
			Threshold
		Default deny	Modelagem séries estado
Assinatura	**Programado**	Modelagem por estado	Transição por estado
			Petri Net
		Sistema especialista	NIDES e EMERALD
		String-matching	NSM A.6
		Baseado em regras simples	NADIR A.7

7.1.4 Entendendo sobre Alarmes em IDSs

O tratamento de alarmes de um IDS pode tornar-se uma grande dor de cabeça tanto para administradores de segurança quanto para administradores de rede. A grande quantidade de alarmes e a taxa de alarmes falsos requerem tempo e muita experiência por parte dos responsáveis pela sua administração. De tal forma a uniformizar a discussão neste tópico, as seguintes definições são apresentadas:

- Alerta/Alarme: Um alarme identifica que o sistema acaba de ser atacado. Tipicamente alarmes incluem informações de diagnóstico sobre o contexto do ataque ou simplesmente sobre eventos estatísticos ou anômalos;
- Falso Positivo: É um alarme gerado por um IDS no qual ele alerta para uma condição que é na verdade benigna, ou seja, o IDS cometeu um erro.
- Falso Negativo: É um não-evento no qual o IDS deixou de gerar um alarme, quando uma condição de alerta de maior importância está em efeito.
- Ruído: É um alarme no qual o IDS envia um alerta sobre uma condição que não é ameaçadora ou não aplicável ao site que está sendo monitorado, mas que foi corretamente diagnosticado. O IDS não cometeu um erro, mas o alarme é de valor questionável.
- Nível de confiança: Este valor pode ser incluído no alarme para indicar a certeza aproximada do IDS de que ele tenha identificado e detectado corretamente um ataque.
- Filtragem de alarmes: Permite que o administrador possa selecionar determinados alarmes e, então, descartá-los com base na configuração do site. Isto se constitui no mecanismo primário para reduzir o número de "falso positivo". Em geral, alarmes são descartados com base no tipo, severidade, valor de confiança, endereços IP destino, endereço IP fonte, tipo de sistema operacional, etc.

Segundo a referência [121], o maior fator de confusão acerca do número de Falso Positivo é a sua relação com o ruído. Em geral quando administradores de sistema reclamam acerca do número de Falso Positivo em geral a verdadeira causa é a geração de ruído.

A referência [122] aponta os seguintes problemas ligados à ocorrência de Falso Positivo:

- O número de alertas coletados por um IDS é relativamente grande, podendo atingir 15000 alarmes por dia por sensor;
- O Número de Falso Positivo é muito alto, podendo chegar a milhares por dia;
- Reduzir a taxa de Falso Positivo em geral leva a perda da confiabilidade do IDS;
- A tarefa de filtragem e análise dos alertas deve ser feitos manualmente;

Segundo os autores, estes problemas fazem com que o usuário final, no caso o gerente de segurança, tenha uma sobrecarga de trabalho para reconhecer ataques verdadeiros dos erros provocados pelo IDS, não tenha confiança nos alertas, e pior, diminua o nível das defesas para reduzir o número de Falso Positivo. Considerando que num ambiente de rede pode-se observar a reação de um sistema monitorado examinando-se os dados de saída dos sistemas em resposta a uma solicitação externa e que os IDSs atuais consideram somente as requisições de entrada de sistemas monitorados, os autores então, sugerem que para melhorar a precisão do IDS de detectar ataques reais, há necessidade de introduzir uma correlação entre os dados que chegam e os que saem, confirmando que o ataque está se realizando antes de ativar um alarme. Em geral todos os ataques reais modificam o fluxo de informações entre o sistema monitorado e os sistemas com os quais eles estão conversando. Por exemplo:

- Ataques de interrupção: Quando um ataque produz a interrupção de um ou mais serviços num sistema, ou mesmo uma falha do sistema, todas as comunicações

são interrompidas. Portanto, observando-se a saída do tráfego da rede, constata-se que não haverá mais dados saindo do sistema monitorado;

- Ataques de percepção: Acesso não autorizado a um sistema é a forma mais comum de se obter informações classificadas. Se uma tentativa é feita, e o sistema reage negando o acesso à informação, alguma forma de mensagem de erro será enviada;
- Ataques de modificação: Quando ataques produzem a modificação da informação fornecida pelo sistema, o comportamento do sistema será alterado, causando a alteração do seu fluxo normal de informação;
- Ataques de fabricação: Se alguém ganha acesso ao sistema e insere falsos objetos, a autenticidade do sistema ficará degradada. Isto produz um desvio do comportamento habitual do sistema, refletindo na alteração da saída usual do próprio sistema.

Na conclusão dos autores a validação do tráfego de saída para um sistema é mais complexo que a validação do tráfego de entrada, pois a ferramenta de correlação terá a função de associar corretamente a entrada suspeita com a resposta apropriada. Neste caso ferramentas baseadas em assinaturas não são adequadas, mas sim as ferramentas de detecção de anomalias, pois elas se adaptam as especificidades do processo de inspeção do tráfego de saída. O artigo apresenta duas ferramentas que realizam esta validação de tráfego: POSEIDON e APHRODITE, ambos usando diferentes técnicas para implementar a ferramenta de correlação. Resultados de benchmark das duas ferramentas são apresentados, demonstrando sucesso no intento de diminuir a taxa de Falso Positivo.

A definição de como o desempenho da detecção, ou precisão, destes sistemas é medido é um ponto crucial para o projeto e implementação de IDSs. No nível mais básico, precisão mede o quanto melhor um IDS detecta ataques. Existem vários componentes de uma medida de precisão [130]. Um deles é a taxa de detecção, que é a porcentagem de ataques que um sistema detecta. Outro componente é a taxa de Falso Positivo. Estas quantidades são medidas testando o sistema para um conjunto de dados (normal e com invasões) previamente escolhidos como o DARPA KDD-99 [131].

7.2 TRABALHOS REALIZADOS

Uma significante quantidade de pesquisa tem sido feita na área de detecção de intrusão ao longo destes 20 anos [103]. Uma boa descrição sobre invasões e detecção de invasões pode ser achada em [83]. O artigo começa com uma discussão sobre atividades intrusivas e tipos de falhas ou vulnerabilidades existentes em sistemas computacionais que permitem a existência destas atividades. A seguir o autor desenvolve um ótimo histórico sobre detecção de intrusão, ilustrado com descrições de sistemas do passado e de interesse atual. Com a visão histórica para fornecer perspectiva, o artigo examina a fundo as tecnologias envolvidas na detecção de intrusão, considerando tanto as forças como as fraquezas. Também são descritos sistemas comerciais, de domínio público e aqueles resultantes de pesquisas. Já a referência [133] fornece uma leitura obrigatória sobre práticas de Detecção de Intrusão, relacionando produtos comerciais, de pesquisa, de domínio público e de iniciativas governamentais, além de uma extensa referência bibliográfica com uma seleção de literatura de IDS por área de interesse. São abordados de forma bastante didática os itens sobre o estado atual das tecnologias de detecção de intrusão, dificuldades atuais e futuras direções, problemas organizacionais como

políticas de segurança e próximos passos recomendados para grupos de pesquisa e pesquisadores, usuários e desenvolvedores de sistemas.

Como já mencionado, existem três tipos de IDSs, vistos sob a perspectiva de arquitetura, baseado em redes, baseado no "*host*" e baseado na aplicação. Algoritmicamente existem dois modelos: detecção de abuso ou baseado em assinaturas e detecção por anomalia. Muitos trabalhos realizados no campo da detecção de anomalias têm procurado determinar um "perfil" para o comportamento do usuário. As invasões são caracterizadas quando um usuário se desvia deste padrão. Estas anomalias são detectadas usando perfis estatísticos [97], geração de padrões indutivos ou redes neurais [104, 105]. A geração de perfis de usuários por tais métodos requer o exame das ações de cada usuário. O modelo adaptativo é vagaroso, pois requer mudanças dos perfis gradualmente para acomodar mudanças no comportamento do usuário. Mudanças repentinas no comportamento são identificadas como irregulares e definidas como intrusão. Em alguns casos, estas anomalias podem ser somente operações normais e que exibiram um comportamento ainda não previsto. Em tais casos, estas anormalidades são indicadas como "falso positivo".

O IDES ("Intrusion Detection Expert System"), projetado pelo SRI International, é considerado um dos primeiros e mais importantes esforços na pesquisa de IDS. Este trabalho foi resultado do artigo de Dorothy Denning, apresentado no IEEE Security and Privacy Symposium em 1986 [106] e subsequentemente re-elaborado em 1987 [96]. O modelo IDES é baseado na hipótese de que é possível estabelecer perfis para caracterizar interações normais de entidades (usuários) com objetos (arquivos, programas ou dispositivos). Os perfis na verdade são modelos estatísticos do

comportamento das entidades e as tentativas do sistema de detectar comportamentos anômalos. Os perfis possuem propriedades estáticas (estáveis) e dinâmicas (determinadas em pequenos intervalos de tempo), de tal forma a permitir que o sistema acomode as mudanças do comportamento do usuário. Estes perfis são suplementados por um sistema especialista que usa regras que descrevem as atividades que representam as violações de segurança conhecidas. Isto impede que o usuário possa treinar o sistema gradualmente para aceitar comportamentos ilegais como normais.

Uma das técnicas usadas para detecção de anomalias é a construção de modelos estatísticos usando métricas derivado da observação da ação dos usuários [107]. Um modelo alternativo é sugerido por [108]. Ao invés de tentar construir perfis normais, os autores focalizam na determinação de comportamento normal para processos privilegiados, como aqueles que executam como "*root*". Outro modelo sugerido por [104] é similar ao anterior, pois ele também considera os processos executados pelo "*root*". A diferença está no uso de uma representação mais simples do comportamento normal, baseando-se em exemplos de execução normal, ao invés de especificação formal de um comportamento esperado do programa. Eles ignoram valores de parâmetros. Este modelo não tem que determinar uma especificação comportamental do código do programa, pois ele simplesmente acumula os traços ("*traces*") de sua execução normal. Ele é capaz de detectar várias intrusões bastante comuns, envolvendo "*sendmail*" e "*lpr*".

Os esquemas de detecção de anomalias também usam técnicas de "*data mining*", tais como "*clustering*", "*support vector machines – SVM*" e diferentes modelos de redes neurais. Por exemplo, [109] descreve o modelo para detecção de intrusão usando

redes neurais e SVM. As principais idéias deste trabalho são descobrir padrões de características que descrevem o comportamento do usuário num sistema e usar o conjunto de características relevantes para construir classificadores que podem reconhecer anomalias e intrusões conhecidas em tempo real. O trabalho compara o desempenho do sistema usando redes neurais e do sistema com SVM usando o conjunto de dados do benchmark KDD (*Knowledge Discovery and Data Mining*) [110], projetado pelo DARPA. Os registros de dados contêm características extraídas do tráfego em conexões de rede utilizado no programa de avaliação de detecção de intrusão do DARPA em 1998 (http://ideval.ll.mit.edu).

A referência [103] introduz o uso de uma rede multiníveis hierárquica Kohonen (K-MAP). Os autores fizeram o treinamento da rede e os testes usando o KDD pré-processado. O objetivo era detectar o maior número possível de ataques. O artigo apresenta o algoritmo de treinamento e a implementação do K-MAP para o IDS. Os resultados mostraram que a taxa de falso-positivo é reduzida significantemente na estrutura K-MAP hierárquico em relação ao modelo K-MAP de camada única em todos os testes. A inovação deste método reside nos seguintes aspectos: O modelo usa a forma mais simples de K-MAP que utiliza poucos recursos computacionais para sua implementação. Além disso, a implementação do K-MAP hierárquico permite a seleção de diferentes combinações de subconjuntos de características com uma ampla faixa de seleção para o número de neurônios usados em cada nível assim como para o limite de treinamento. Baseado nos testes que foram realizados, foi obtido taxas de detecção da ordem de 90,94% e 93,46% e taxas de falso-positivo entre 2,19% e 3,99%. Estes resultados são melhores que os trabalhos anteriores utilizando outros algoritmos.

Na referência [111], é apresentado um algoritmo de "*data mining*" baseado em "*Supervised Clustering*" para aprender padrões e usar estes padrões para classificação de dados. O algoritmo desenvolvido permite a aprendizagem incremental escalável de padrões de dados com variáveis numéricas e nominais. A versão estendida do algoritmo de "*data mining*", "*clustering and classification algorithm – supervised ECCAS*" permite o tratamento de diferentes tipos de dados. Neste estudo aplicou-se ECCAS em três conjuntos de dados para detecção de intrusão, diagnóstico médico e de salário, respectivamente, cada um com tipos de dados misturados, para avaliar a precisão da classificação e confiabilidade de ECCAS. O problema de detecção de intrusão pode ser considerado como um problema de classificação nos quais dados de atividades de computadores e redes são monitorados e classificados em uma das duas classes: normal ou anômala (intrusiva). Mais classes poderiam ser utilizadas se uma classificação mais fina fosse necessária, por exemplo, com diferentes tipos de ataques. Dois tipos de dados de atividades do sistema são usualmente utilizados para detecção de intrusão: Registtro (log) do tráfego de dados do computador e da rede ou os dados de auditoria do sistema. Neste estudo foi usado o benchmark KDD. Os dados para treinamento incluíram 500.000 registros de conexões de sete semanas de tráfego de rede. Os dados de testes incluíram cerca de 300.000 registros de conexões. Uma conexão contém uma seqüência de pacotes TCP dentro do tempo definido para o fluxo de dados do endereço IP fonte para um endereço IP destino, usando um protocolo de aplicação. Para cada conexão, foram extraídas características dos registros da conexão para ajudar a distinguir entre as conexões normais das conexões intrusivas. Portanto, cada registro de conexão nos dados de treinamento terá o valor da variável "*target*" conhecida como normal ou intrusivo acompanhada pelo tipo de ataque específico. Ataques caem em 4 categorias: atividade normal, supervisão, DoS e acesso não autorizado de máquina remota. Dois diferentes

métodos de ECCAS foram avaliados. Ambos os métodos produziram desempenho satisfatório para o mesmo conjunto de dados.

A referência [112] apresenta os resultados da pesquisa sobre detecção de ataques em redes de computadores e de sistemas de controle através da identificação e monitoramento de uma "Seqüência de DNA" sintético. Assim como o DNA caracteriza a composição do corpo humano, e o funcionamento anormal dos tecidos pode ser reconhecido como uma seqüência alterada de DNA, uma "Seqüência de DNA" de um sistema computacional tem funções similares. Mudanças nos padrões de comportamento deste sistema, tal como ataque de vírus, são refletidos em mudanças na "Seqüência de DNA" e ações apropriadas devem ser tomadas.

Deste modo, o problema de segurança será definir o que a seqüência de DNA deveria parecer e como monitorar sua evolução. O objetivo da pesquisa está em definir uma seqüência de DNA para cada atividade (por exemplo, tráfego TCP/IP) e o monitoramento de sua evolução. O artigo descreve os esquemas de tratamento das mudanças da seqüência DNA, o qual resultará em operações legítimas ou em ataques maliciosos. Os autores relatam como a tecnologia pode ser aplicada ao ambiente de controle de processo onde temos controladores de processo equipados com servidores HTTP para acesso a dados. Tais ambientes são vulneráveis a ataques internos e externos e forneceram um excelente banco de testes para esta pesquisa. Pesquisas na área Detecção de Intrusão têm focado principalmente no monitoramento estático da integridade do sistema, usando regras predefinidas, assinaturas e padrões de comportamento. Estes métodos são úteis para reconhecer e impedir ataques conhecidos, mas são absolutamente sem utilidade contra novas formas de ataque. A questão básica

colocada pelos autores é se existem maneiras de caracterizar sistemas dinâmicos (hardware, software e usuários) de tal forma que qualquer interrupção do sistema pode ser facilmente detectada. A idéia sugerida para esta questão foi o uso da técnica do "*footprinting*", utilizada pelos "hackers" para coletar informações antes de atacar [113]. Desta forma os dados coletados pelo "*footprinting*" são filtrados e utilizados para definir uma assinatura dinâmica do sistema monitorado. Esta assinatura evolui com o tempo, baseando-se nos padrões de uso do sistema e nas mudanças do sistema da mesma forma que a seqüência de DNA proposta. Portanto, o primeiro requisito na definição das seqüências de DNA é capturar as características essenciais de um sistema para uma determinada aplicação ou um grupo de usuários. A lista de categorias de um sistema computacional que necessitam ser monitoradas inclui: tráfego da rede, sistema de arquivos e arquivo de dados. Para cada categoria um determinado número de características deve ser capturado. Por exemplo, para tráfego da rede deve-se capturar o volume de tráfego, o protocolo usado, o tamanho do pacote e endereço IP. O escopo da detecção de mutação de DNA na pesquisa foi limitado ao tráfego de rede. Este estudo foi extendido para sistemas de controle industrial onde CLPs estão conectados em uma rede Ethernet. Uma conclusão importante deste trabalho foi a constatação de que o monitoramento de seqüências de DNA usando o tráfego de redes de sistemas de controle de processo é mais simples do que o tráfego de redes corporativas.

A referência [114] propôs um modelo de identificação de intrusão para redes em tempo real usando "*Principal Component Analysis - PCA*". Esta técnica é utilizada para criar um perfil de comportamento normal de programas e usuários para detecção de intrusão por anomalia baseado em "*host*". A inovação desta técnica reside em dois fatores: Primeiro, o modelo não somente detecta, mas identifica as invasões pelo perfil

normal de comportamento da rede, bem como pelos perfis de comportamento de vários ataques. Em segundo lugar, o modelo pode obter a identificação da invasão em tempo real, baseado na redução dimensional e no uso de um classificador mais simples.

No método proposto cada conexão de rede é transformada em um vetor de dados de entrada. PCA é usado para reduzir as dimensões dos vetores de dados e a identificação é tratada dessa forma num espaço dimensional com maior eficiência e baixo uso de recursos computacionais. O modelo foi testado com dados de rede do MIT Lincoln Labs para o "*1998 DARPA Intrusion Detection Evaluation Program*" e os resultados mostraram que o método é promissor em termos de precisão da identificação e eficiência computacional para identificação em tempo real. A avaliação do desempenho do método é comparada com outros 5 métodos descritos no artigo.

A referência [115] introduz o algoritmo hierárquico de seleção de subconjuntos aleatórios/seleção de subconjuntos dinâmicos (RSS-DSS), para filtrar dinamicamente grandes conjuntos de dados baseados em conceitos de treinamento de padrões de período de tempo e dificuldade, enquanto utilizando uma estrutura de dados para facilitar o uso eficiente da memória hierárquica. Tal esquema fornece a base para treinar a programação de algoritmos genéticos num conjunto de dados de meio milhão de padrões em 15 minutos. O método foi demonstrado no conjunto de dados para detecção de intrusão KDD-99, com resultados similares àqueles identificados na competição KDD-99 original. Parâmetros do RSS-DSS demonstraram ter uma boa efetividade numa larga faixa de valores.

A referência [116] apresenta duas técnicas hibridas para modelar IDSs. Árvores de decisão (DT) e "*support vector machines*" (SVM) são combinados como um modelo hierárquico de sistema inteligente hibrido (DT-SVM) e um modelo conjunto combinando os classificadores base. O modelo de sistema de detecção de intrusão hibrido combina classificadores base e outros paradigmas de aprendizagem híbridos a fim de maximizar a precisão da detecção e minimizar a complexidade computacional. Resultados empíricos apresentados ilustram que o sistema híbrido proposto alcança tais objetivos. O artigo apresenta, também, uma revisão da literatura sobre paradigmas de aprendizagem de máquina aplicados a sistemas de detecção de intrusão.

Como já descrito em capítulos anteriores, sistemas SCADA representam uma vulnerabilidade para infra-estruturas críticas. Desta forma os Sistemas Elétricos de Potência estão sujeitos a invasões através seus sistemas SCADA. Em [117], os autores alegam que a própria instrumentação fornece variações detectáveis em resposta a tais interferências. O artigo apresenta, então, uma estratégia que melhora o método de estimação de estado usando sistemas fuzzy híbridos para monitoramento de faltas e diagnósticos, com o objetivo de combinar informações de múltiplos domínios de modo a detectar, isolar, identificar e mitigar as ameaças contra o sistema elétrico como um todo. De tal forma a dotar os métodos de solução por estimação de estado com certo grau de robustez numérica, o "*algorithm-based error detection – ABED*" é aplicado ao procedimento de eliminação gaussiana. Resultados da simulação revelaram que ABED fornece detecção de erro com baixo custo e excelente cobertura para aritmética em ponto-flutuante sem a ocorrência de falsos alarmes.

CAPITULO 8

DETECÇÃO DE ATAQUES POR ANOMALIA EM SISTEMAS ELÉTRICOS DE POTÊNCIA USANDO TÉCNICAS INTELIGENTES

O Capítulo 6 salientou a importância dos sistemas SCADA na infra-estrutura de energia elétrica, bem como sua vulnerabilidade. Já o Capítulo 7, estudou como melhorar a segurança de sistemas de informação usando Sistemas de Detecção de Intrusão. Neste mesmo capítulo são apresentados diversos trabalhos que utilizam diferentes modelos para realizar o algoritmo de detecção proposto. Muitos deles utilizam técnicas inteligentes para realizar a tarefa de análise, como "*Data Mining*", sistemas baseados em regras, sistemas especialistas, redes neurais, etc. No caso de sistemas de controle que utilizam sistemas SCADA, em geral utiliza-se dois modelos de detecção de intrusão para melhorar a segurança dos sistemas de informação: O primeiro identifica ataques que utilizam a infra-estrutura de comunicações, como a maioria dos casos descritos no Capítulo 7, e o segundo modela o fluxo de dados e as operações de controle em sistemas SCADA para detectar anomalias causadas por tentativas de mudar ou causar prejuízos ao sistema como descrito em [117]. Este capítulo faz um estudo dos trabalhos publicados nesta área e que orientaram a proposição do modelo de detecção de anomalias usando técnicas inteligentes para sistemas de informação de sistemas elétricos de potência.

8.1 TRABALHOS PUBLICADOS

A referência [6] descreve o desenvolvimento do projeto SAFEGUARD (http://www.elec.qmul.ac.uk/safeguard/) cujo objetivo é melhorar a dependência e sobrevivência de grandes infra-estruturas críticas através do monitoramento e proteção usando agentes autônomos. Em geral os objetivos de segurança integridade e disponibilidade em infra-estruturas críticas são monitorados e mantidos por operadores. O Projeto SAFEGUARD utiliza tecnologia de agentes para o desempenho das funções de controle automático e auxiliar os operadores a tomar decisões corretas no momento certo. Em sua arquitetura, o projeto combina detecção baseada em conhecimento e detecção baseada em comportamento num modelo de detecção hibrida que nivela o conhecimento existente e busca desvios significantes da normalidade da operação do sistema.

O modelo é implementado por agentes com tipo de dados voltado para os domínios da telecomunicação e de sistemas elétricos de potência. Por exemplo, um agente poderia estar monitorando pacotes IP, enquanto outro verifica diferenças de temporização em sistemas SCADA e outro examina as leituras de potência da rede elétrica. A detecção é projetada para ser utilizada nos níveis inferiores da estrutura do sistema. A segunda fase na identificação dos problemas é a correlação destas informações para formar a base de uma resposta combinada. É estratégia do SAFEGUARD utilizar agentes distribuídos para realizar esta correlação de eventos para o operador. A arquitetura do projeto é apresentada na Figura 8.1. Desta figura destacamos o bloco do Agente de Detecção Hibrida ("*Hybrid Detector Agent*") e o bloco do Agente de Correlação. O Agente de Detecção Hibrida monitora os dados da rede elétrica e procura identificar a corrupção da informação usando uma combinação

de métodos de detecção de assinaturas e anomalias. O Agente de Correlação coleta a informação de outros agentes, como o de Detecção Hibrida, faz aproximações de hipóteses sobre o estado do sistema e sugere uma resposta apropriada.

O desafio desta correlação no domínio do Sistema Elétrico de Potência é a complexidade do sistema e o grande número de cenários possíveis. Diversos trabalhos publicados no âmbito deste projeto envolveram o Queen Mary, University of London, Aplicaciones em Informática Avanzada, ENEA, Linköping University e Swisscom.

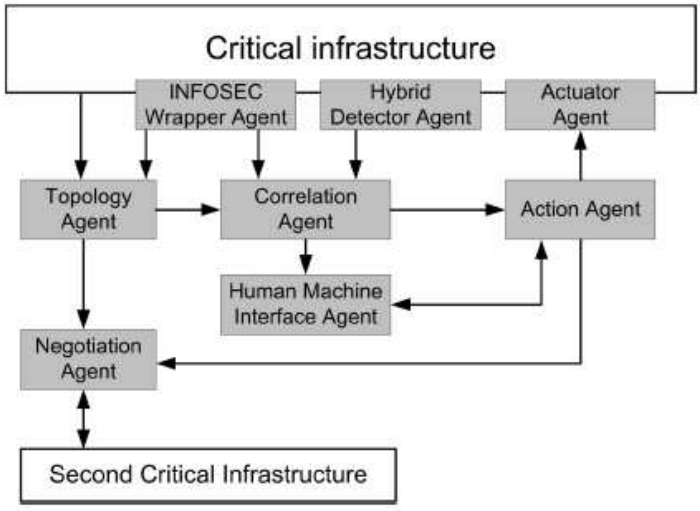


Figura 8.1 - Arquitetura do Projeto SAFEGUARD.

Na referência [123], é apresentado com que precisão e segurança os sistemas SCADA podem ser melhorados utilizando a detecção de anomalias para identificar valores falsos produzidos por ataques e faltas. O artigo utiliza dados oriundos do Sistema Elétrico de Potência para demonstrar o desempenho de dois métodos de detecção de anomalia: Indução Invariante e N-Gram. Por considerar uma área de pesquisa promissora, os autores utilizaram o modelo de detectar anomalias do fluxo de dados e dos sinais de controle do sistema SCADA, ao invés monitorar o comportamento do sistema por meio de seqüências de chamadas de funções e conexões entre as máquinas.

O modelo escolhido tem a vantagem de detectar ataques desconhecidos e ações maliciosas de pessoas de dentro da organização, embora possa gerar muitos falsos alarmes se não tratado com o devido cuidado. As técnicas descritas no artigo fazem parte do projeto IST SAFEGUARD [6] e foram incorporadas dentro de agentes que são utilizados para detectar e reparar anomalias dentro de grandes e complexas infra-estruturas críticas.

Como já mencionado anterioremente, a rede de um sistema elétrico de potência é controlada pela troca de sinais de controle entre os centros de controle e as UTRs, que por sua vez controlam os disjuntores, os transformadores, as chaves seccionadoras, etc. As tarefas de aquisição dos dados e do controle supervisório são executadas por meio de sistemas SCADA. Os dados coletados por estes sistemas são incompletos e sujeitos a estarem corrompidos ou perdidos. Uma aplicação chamada Estimador de Estados é utilizada para lidar com estes problemas. Como o Estimador de Estados não consegue trabalhar bem com grande perda de dados, ele assume que sua informação sobre a rede elétrica é sempre correta. Esta é uma hipótese de risco, pois em geral existem erros de configuração e há sempre a chance de que um atacante poderia estar mediando entre o centro de controle e o sistema elétrico (como em "*man-in-the-middle"*).

As duas técnicas abordadas no texto são utilizadas para modelar sistemas SCADA em redes do sistema elétrico de potência: Uma técnica trata os dados como texto e aprende os padrões normais exibidos pelo texto (N-Gram); A outra técnica trata os dados como números e procura por invariantes, tais como relações matemáticas entre números (Indução Invariante). A técnica N-Gram, desenvolvida por Marc Damaschek, foi modificada para ser aplicada em dados oriundos de sistemas elétricos de potência. Ao invés de tolerar os erros, em sistemas elétricos de potência é necessário detectá-los. Em medidas elétricas a falta do ponto decimal ou a troca de sinal do valor medido

resulta numa leitura totalmente diferente. Esta técnica é bem tolerante ao erro porque é essencialmente uma técnica estatística que mede as distribuições de N-Gram nos dados.

A técnica de Indução Invariante constrói o modelo normal de dados procurando relações entre diferentes leituras. Estas relações são expressas como invariantes, por exemplo, fatos que devem sempre manter o contexto atual. Nos dados presentes em redes elétricas, este modelo é particularmente efetivo, pois muitos dos dados são interrelacionados de maneira sistemática. Através de uma aplicação de fluxo de carga, as medidas de potências ativas e reativas para uma rede de 6 barras foram calculadas e as cargas do sistema total para um ciclo anual dado usando a especificação da rede de teste de 24 barras ("*IEEE Reliability Test System*"). Isto produziu 8736 arquivos contendo leituras da rede para cada hora de cada dia do ano.

Para testar a taxa de falso positivo dos detectores de anomalias, um entre dez destes arquivos foi escolhido e, então, as técnicas de N-Gram e Indução Invariante foram usadas para aprender o modelo normal da rede. Em seguida foi introduzido de 1 a 44 erros, tais como troca de sinal, movimentar o ponto decimal e troca de dígitos aleatoriamente, em cada um dos arquivos selecionados. A capacidade de identificar erros pelas duas técnicas foi avaliada. Foram conduzidos dois experimentos utilizando as duas técnicas: o primeiro experimento media as taxas de falso positivo e de valores reais por arquivo. O segundo experimento media a capacidade de identificar erros verdadeiros em cada arquivo corrompido. Ambas as técnicas realizaram bem o primeiro experimento. N-Gram identificou 19,8 % com 1% de taxa de falso positivo. Indução invariante identificou 19,1 % de arquivos corrompidos com 4% de taxa de falso positivo. No segundo experimento a técnica de N-Gram provou ser melhor quando utilizada para identificar um pequeno número de erros dentro de cada arquivo. Mas

quando o número de erros aumentava, as taxas de falso positivo tornavam-se sem significado.

A indução invariante realizou esta tarefa com melhores resultados, ao identificar linhas corrompidas dentro dos arquivos. O resultado destes testes sugere que a melhor forma para detectar anomalias em sistemas elétricos de potência é combinar mais de uma técnica de detecção de anomalia. Um modo efetivo de realizar isto está sugerido em [124], onde os autores utilizam uma rede Bayesiana para correlacionar as saídas com outras fontes de dados. Isto reduziria o número de falso positivo e melhoraria a precisão dos erros.

A referência [125] propõe um modelo para monitorar e proteger sistemas elétricos de potência usando técnicas de aprendizagem do comportamento normal do sistema no nível das subestações e indicando através de sinais de alarme uma condição de anormalidade. As técnicas descritas no artigo fazem parte do projeto SAFEGUARD [6]. O artigo propõe construir um sistema capaz de realizar monitoramento online em subestações que fazem parte de um sistema elétrico de potência, ler medidas das UTRs e informar a ocorrência de eventos anômalos através de um detector de anomalias. Uma das maiores dificuldades encontradas no monitoramento de grandes infra-estruturas críticas é a característica não linear de seu comportamento, obrigando o uso de métodos numéricos que consomem tempo e recursos e não são indicados para um monitoramento online.

Segundo os autores as peculiaridades exibidas pelos sistemas elétricos de potência e as características específicas do problema sugerem o uso de redes neurais para o monitoramento contínuo dos dados coletados pelos sistemas SCADA. O modelo utiliza um "*autoencoder*" para cada subestação. O "*autoencoder*" é um "*Autoassociative Neural Network Encoder*" que exibe 2 características principais: a Autoassociatividade

e a Camada Gargalo ("*bottleneck layer*"). Devido às particularidades de cada subestação em termos de seus componentes, localização geográfica, função de transmissão e/ou distribuição, é necessário ter um treinamento específico para cada rede neural empregada. A arquitetura do sistema de detecção de anomalias proposto é apresentada na Figura 8.2. A função de pré-processamento organiza os dados para cada "*autoencoder*" em janelas de tempo deslizantes. O "*autoencoder*" adequadamente treinado é capaz de reproduzir o conjunto de dados considerados como comportamento normal.

O pós-processamento, através da técnica de "*novelty assessment*", identifica um novo valor, que o sistema de aprendizagem não está informado pelo treinamento [127]. Nesta técnica entradas "negativas" são reconhecidas como sendo de natureza diferente – anormal - ("*novel*") comparada com as entradas positivas, consideradas normais e que são mais familiares, pois elas pertencem à classe que foi usada para treinamento. Desta forma "*novelty detection*" difere-se de outras técnicas convencionais de classificação, pois ela tenta reconhecer a amostra de certo conceito ao invés de diferenciá-la entre amostras de ambas as classes [128].

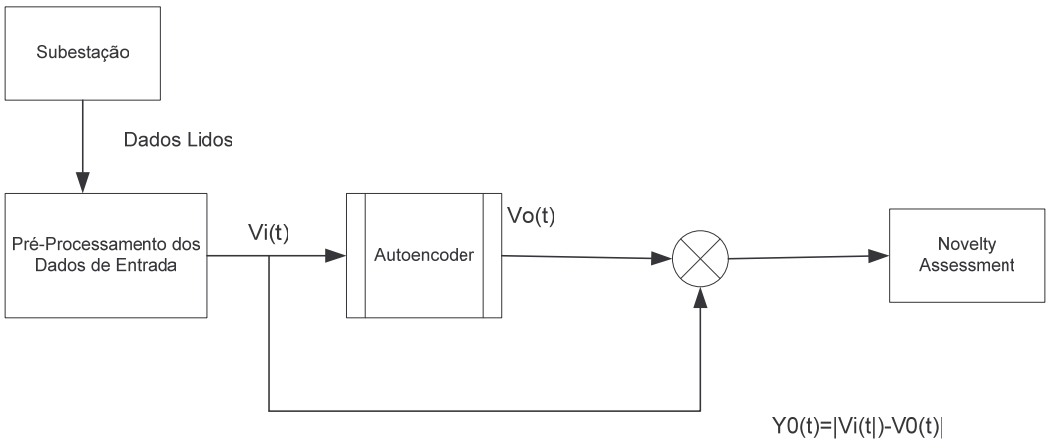


Figura 8.2 - Arquitetura do detector de anomalias.

Os valores limites ("*threshold*") são definidos para o comportamento normal do sistema e utilizados para indicar a ocorrência ou não de uma condição anormal indicada por um alarme. Os resultados experimentais foram conduzidos implementando-se o modelo de sistema elétrico IEEE RTS-96 [126] em um simulador de redes elétricas. O treinamento, usando um algoritmo de "*backpropragation*" levou 72 horas, consistindo de 432 padrões de treinamento. Para testar o autoencoder com valores não-normais foram feitas as seguintes modificações no conjunto de dados original: introdução de ruído aleatório em cada vetor de medidas, mudanças no formato da curva de demanda de carga e mudanças na topologia da rede elétrica ou o estado de componentes.

Estas mudanças visam simular erros nas medidas dos sensores ou alteração intencional de dados, faltas intencionais ou não, em componentes da rede elétrica, interrupção de linhas de transmissão e tendência de demanda de carga não esperada. Os resultados obtidos e demonstrados no artigo provaram que o modelo proposto detectou com sucesso as anomalias simuladas. Após o treinamento dos dados relativos à atividade normal dos componentes, o "*autoenconder*" tornou-se capaz de mapear o comportamento do sistema.

8.2 ALGORITMO DO DETECTOR DE ANOMALIAS

A base do detector de intrusão por anomalias proposto é o algoritmo de conjuntos aproximados. Nesta seção faremos uma breve introdução do algoritmo e como ele é utilizado para implementar o detector de intrusão.

8.2.1 Teoria dos Conjuntos Aproximados

A Teoria de Conjuntos Aproximados foi proposta em 1982 por Z. Pawlak [136]. A idéia fundamental desta teoria é achar um conjunto que represente os exemplos (conjunto de dados) através de dois conjuntos de aproximação, um superior e outro inferior. Assim, através dos conhecimentos disponíveis nos exemplos, o conjunto de aproximação superior deve ser reduzido; enquanto através deste mesmo conhecimento o conjunto de aproximação inferior deve ser expandido.

Neste trabalho, a idéia será representar o conjunto final através de um conjunto de regras de produção, que consigam detectar invasões no sistema.

Um sistema de informação pode ser definido como sendo uma 4-upla na forma K=(U,R,V,ρ), onde U é um conjunto finito de objetos (espaço de busca), R é um conjunto finito de atributos (tipo de palavras (*strings*), estado dos equipamentos e linhas, entre outros), V é o domínio de cada atributo de R, e ρ é uma função total (chamada de função de informação) que define a seguinte aplicação: ρ:U×R→V, isto é, os exemplos.

O conceito de sistema de informação não é exclusivo da Teoria de Conjuntos Aproximados e tem utilização extensiva em Teoria de Informação. Uma das maiores contribuições da Teoria dos Conjuntos Aproximados é transformar automaticamente dados em conhecimento [137].

Como dito anteriormente, esta teoria trabalha com conjuntos de aproximação superior e inferior, denotados por $\overline{R}X$ e $\underline{R}X$. Assim três regiões são criadas e denominadas de: região positiva, $POS_R(X)$, região fronteira, $BN_R(X)$, e região negativa, $NEG_R(X)$, conforme mostrado na Figura 8.3. A seguir, estas regiões são definidas matematicamente.

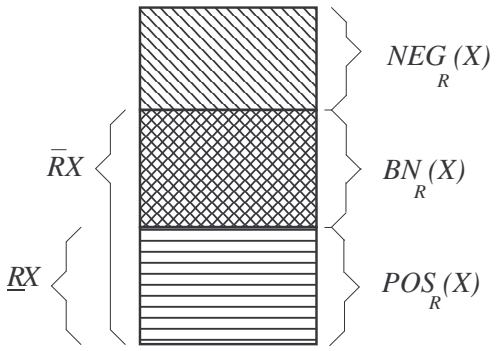


Figura 8.3 – Definição dos Conjuntos Aproximados de R e suas regiões de interesse.

Seja o conjunto $X \subseteq U$, e R uma relação equivalente, e $K = (U,\{R\})$, uma base de conhecimento. Desta forma, dois subconjuntos podem ser associados por:

a) R-inferior: $\underline{R}X = \cup \{Y \in U/R : Y \subseteq X\}$

b) R-superior: $\overline{R}X = \cup \{Y \in U/R : Y \cap X \neq \emptyset\}$

Estas definições indicam que todos os elementos que pertencem ao conjunto $\underline{R}X$ (aproximação inferior) com certeza pertencem a solução procurada; enquanto os elementos do conjunto $\overline{R}X$ (aproximação superior) podem pertencer a solução.

Desta forma, pode-se definir as áreas $POS_R(X)$, $BN_R(X)$ e $NEG_R(X)$:

c) $POS_R(X) = \underline{R}X \Rightarrow$ com certeza membro de X

d) $NEG_R(X) = U - \overline{R}X \Rightarrow$ com certeza não é membro de X

e) $BN_R(X) = \overline{R}X - \underline{R}X \Rightarrow$ possível membro de X

8. 2.2 Algoritmo de Conjuntos Aproximados

Existem dois conceitos importantes que devem ser apresentados antes da apresentação do algoritmo, que são conjunto redução e conjunto núcleo. Seja **R** uma família de relações equivalentes. O conjunto redução de **R**, *RED*(**R**), é definido com um conjunto reduzido de relações que conserva a mesma classificação indutiva do conjunto **R**. O conjunto núcleo de **R**, *CORE*(**R**), é o conjunto de relações que aparecem em todo a

redução de **R**, isto é , o conjunto de todas as relações indispensáveis para caracterizar a relação **R**.

A idéia do algoritmo a ser utilizado é ir simplificando o conjunto de exemplos através de do seguinte procedimento:

a) calcular o conjunto núcleo do problema;

b) eliminar (ou substituir) uma variável usando uma outra; e

c) redefinir o problema usando novas categorias básicas.

Um algoritmo que segue o procedimento acima pode ser representado pelos seguintes passos:

Passo 1: Eliminar os atributos dispensáveis.

Passo 2: Calcular o conjunto núcleo de cada exemplo.

Passo 3: Recompor a tabela de exemplos com os valores de redução.

Passo 4: Juntar possíveis exemplos redundantes.

CAPITULO 9

EXPERIMENTOS E RESULTADOS

9.1 COMUNICAÇÃO DE DADOS EM SISTEMAS SCADA

Os sistemas SCADA são utilizados para coletar dados de sensores e instrumentos localizados em locais remotos e transmitir os mesmos até um centro de controle para propósitos de controle e supervisão. Estes sistemas podem monitorar e controlar centenas a centenas de milhares de pontos de entrada/saída. As UTRs e CLPs se localizam entre os sensores remotos e o centro de controle com a função de coletar os dados dos sensores e dispositivos de campo, conforme mostrado na Figura 9.1. Os sensores possuem entrada/saída digital ou analógica que não são facilmente transmitidos a longas distâncias. Desta forma as UTRs e CLPs são utilizadas para digitalizar e empacotar os sinais dos sensores de modo que eles possam ser transmitidos digitalmente através do uso de protocolos de comunicação industriais sobre grandes distâncias. Alguns exemplos destes protocolos são: Modbus, DNP 3.0, ICCP. Já os protocolos padrão utilizados pela camada física são do tipo serial, como por exemplo, RS485, RS422 e RS232.

O sistema SCADA fica localizado em um PC industrial, ou estação de trabalho, contendo o software para Interface Homem-Máquina (IHM). Este software é utilizado para ler as estações remotas e armazenar os dados coletados em algum banco de dados

centralizado. Desta forma a aquisição de dados é iniciada primeiramente pelas UTRs ou CLPs, lendo os campos de entrada a eles conectados. Uma vez os dados sejam lidos eles são transmitidos para estação de trabalho onde os dados serão processados. Existem 3 tipos de dados coletados: Analógico, Digital e Pulso (contador).

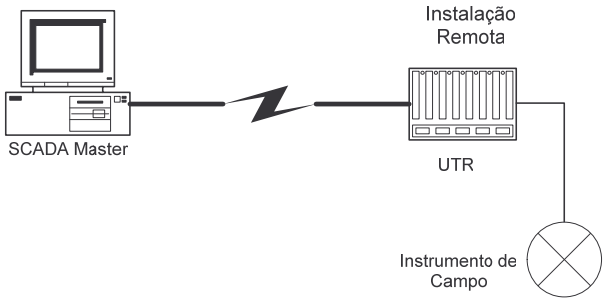


Figura 9.1 - Modelo de comunicação em sistemas SCADA

A comunicação empregada pelo sistema SCADA utiliza diversos meios físicos, tais como linhas públicas, linhas discadas, fibra ótica, ADSL, etc, e meios sem fio (wireless), tais como rádio, "*spread spectrum*", celular (GSM), WLAN, ou satélite, conforme mostrado na Figura 9.2.

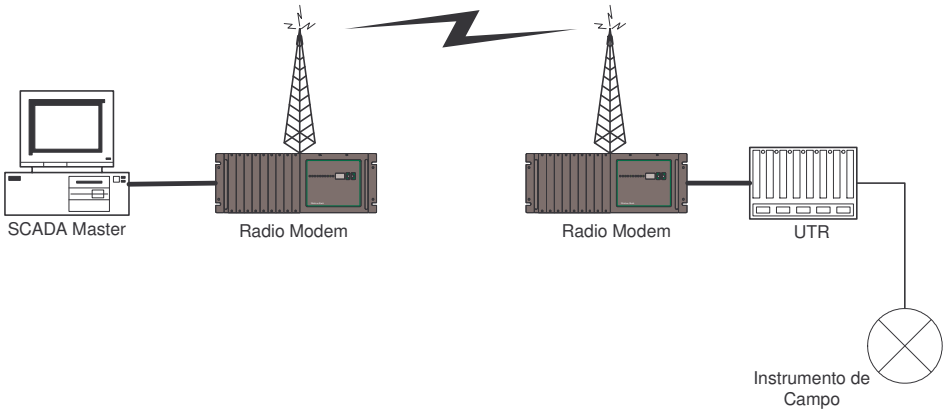


Figura 9.2 - Modelo utilizando radio integrado a UTR.

O padrão IEC61850 "*Communication Networks and Systems in Substations*" [138] define um modelo padrão de arquitetura de comunicação em subestações usando

tecnologia Ethernet e Internet, conforme mostrado na Figura 9.3. No nível da camada de "processo", dados de sensores de corrente e de tensão, bem como informação do estado dos equipamentos são coletados e digitalizados através de "*Merging Units*" (MUs). A partir destas unidades os dados são transferidos para a camada de "subestação" usando tecnologia Ethernet com redundância.

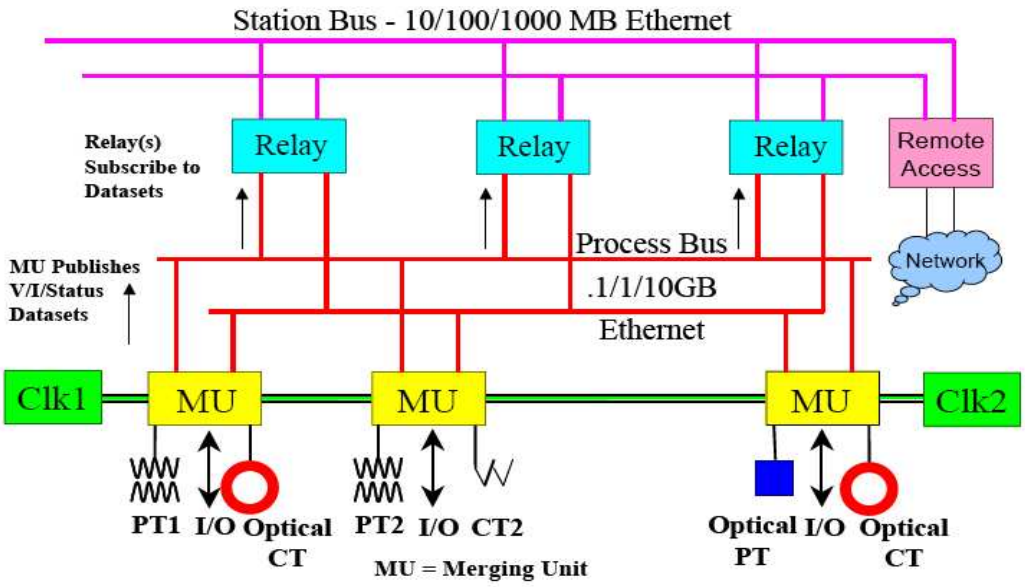


Figura 9.3 - Modelo de comunicação em subestação pelo padrão IEC61850 [138].

No Brasil, os Procedimentos de Rede definem o sub-módulo 10.19 para tratar especificamente dos requisitos de tele-supervisão para a operação. Este sub-módulo define no item 4.3.1 como recurso de supervisão e controle dos Agentes o conjunto formado por:

- Ponto de captação de dados ou de aplicação de comando no campo, ou seja, transdutores, relé de interposição, reguladores de velocidade/potência e outros equipamentos;
- Interligação de dados, ou seja, o conjunto de equipamentos de sistemas que se interponham entre o ponto de captação de dados ou de aplicação de comando no campo e os computadores de comunicação do Centro do ONS.

A Figura 9.4, retirada do Sub-módulo 10.19, apresenta uma interpretação gráfica deste conceito de interligação de dados e dos recursos de Supervisão e Controle do Agente.

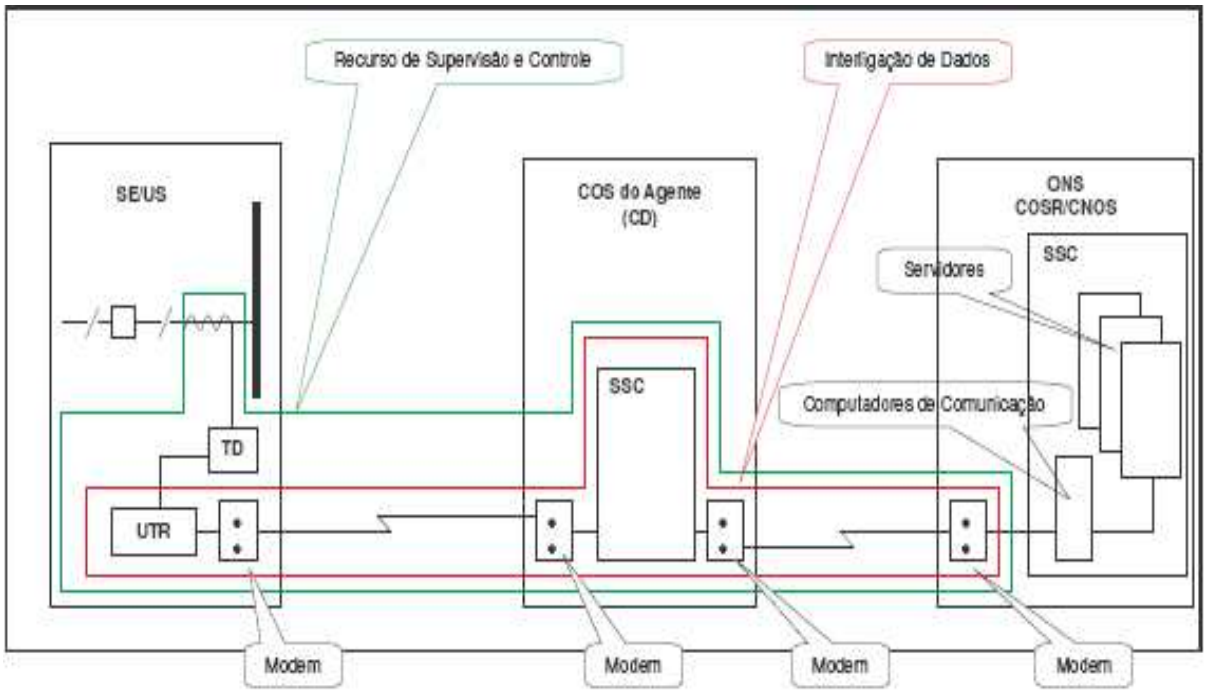


Figura 9.4 - Exemplo de Recurso de Supervisão e Controle

(Fonte: http://www.ons.org.br)

Dentre as principais funções dos centros de operação do ONS, viabilizadas pelos recursos de supervisão e controle dos agentes, estão os sistemas SCADA (Supervisão Controle e Aquisição de Dados), os sistemas de monitoração e controle da geração, os sistemas de monitoração e coordenação do perfil de tensão, as funções de análise de rede, de histórico, etc.

Com relação ao protocolo de comunicação, o sub-módulo determina que ele seja compatível com os atuais protocolos encontrados nos centros de controle designados

pelo ONS. Além disso, o ONS está padronizando o uso dos protocolos DNP 3.0, para conexão com remotas e ICCP (IEC 68850) para interligação com outros centros de controle.

O item 6.2 do referido sub-módulo descreve quais informações cada equipamento da Rede de Supervisão transfere para o centro controlador da área. Dentre as informações podemos citar medições analógicas, como tensão, potência reativa, potência ativa, posição de tap do transformador, corrente e freqüência, sinalização de estado com selo de tempo e seqüenciamento de eventos.

Os recursos de supervisão e controle providos pelos agentes ao ONS deverão ter sua disponibilidade e qualidade medidas de acordo com a metodologia estabelecida no sub-módulo 10.19. Esta avaliação é feita para cada UTR, sistema de supervisão local e concentrador de dados do agente, através de índices agregados a cada um deles.

Os protocolos de comunicação fornecem as regras para que os computadores que ficam localizados remotamente e aqueles localizados nos centros de operação possam trocar dados e sinais de controle. O protocolo define a estrutura e o formato da mensagem e determina como o equipamento remoto, chamado de escravo, reconhecerá as mensagens enviadas pelo computador mestre, e como decodificar a informação contida na mensagem.

Por exemplo, o DNP3 é um protocolo para transmissão de dados ponto a ponto usando comunicação serial e IP e largamente utilizado por empresas de energia elétrica. Muitos fornecedores oferecem produtos que operam usando TCP/IP para transportar

mensagens DNP3. Os quadros da camada de enlace de dados são, então, encapsulados dentro de pacotes TCP/IP. Isto permite que o DNP3 tenha as vantagens oferecidas pela tecnologia Internet, mas com a desvantagem de incorporar as vulnerabilidades presentes nas redes com tecnologia TCP/IP. Lembre-se que este protocolo foi projetado para otimizar a transmissão de dados e sinais de comando, não sendo um protocolo de propósito geral como aqueles encontrados na Internet.

A Figura 9.5 apresenta a relação mestre-escravo ("*Master/Outstation*" na nomeclatura do DNP3), retirada de [139]. A UTR está representada com um conjunto de dados, na forma de vetores, vindos dos sensores e armazenados na base de dados local e de comandos que estão sendo enviados para os dispositivos de saída. O mesmo procedimento ocorre do lado do "*master*", onde ele usa valores presentes na sua base de dados para propósitos específicos, tais como gráficos, análises de tendências, estado dos equipamentos do sistema, alarmes, etc. O objetivo do "*master*" é manter a base de dados atualizada. Desta forma ele envia pedidos de "*request*" para a UTR pedindo para que ela retorne os valores da sua base de dados. Este método é chamado de "*polling*". A UTR responde, enviando o conteúdo de sua base dados. Para o sub-módulo 10.19 dos Procedimentos de Rede do ONS, as medições são feitas de forma individualizada e transferidas periodicamente para os centros de operação. O período de transferência é parametrizável, devendo suportar períodos de pelo menos 4 seg.

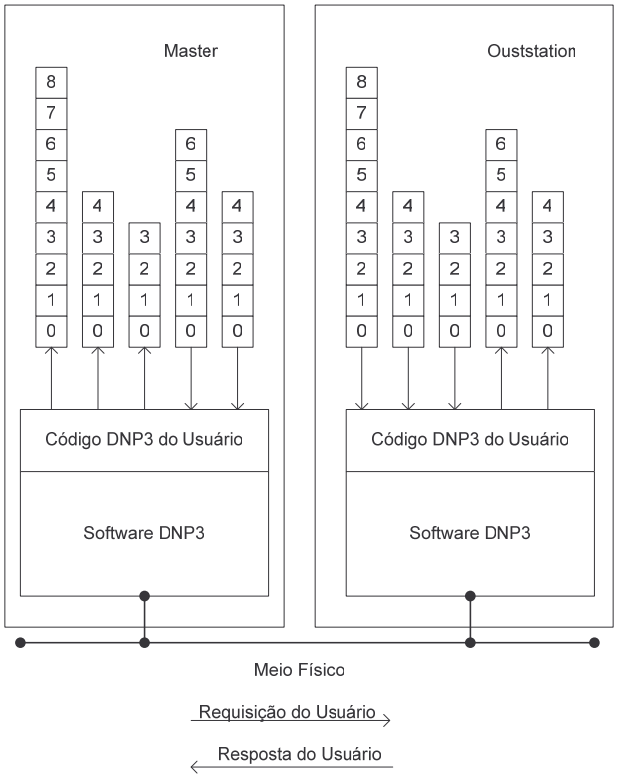


Figura 9.5 - Relação "*master-outsation*" no protocolo DNP3 [139].

O quadro do DNP3 consiste de um cabeçalho e uma seção de dados ("*data payload*"). O cabeçalho especifica o tamanho do quadro, as informações para o enlace de dados e os endereços fonte e destino dos dispositivos envolvidos na conversação. O tamanho máximo da seção de dados é de 250 bytes. O DNP3 pode representar dados em diferentes formatos, tais como valores inteiros de 16 e 32 bits e valores em ponto-flutuante de 32 ou 64 bits.

A Figura 9.6, retirada de [129], apresenta o exemplo de um sistema de controle de uma subestação hipotética. Nesta figura verifica-se as diversas conexões existentes entre os dispositivos elétricos, como transformadores, disjuntores e relés, conectados a suas respectivas UTRs, através de conexão de rede local ou transmissão serial. Estes por sua vez conectam-se com o controlador da subestação através da rede corporativa,

via rede Internet (TCP/IP), ou ao servidor SCADA Master. O Controlador da Subestação conecta-se ao servidor SCADA Master utilizando-se de fibra ótica dedicada, ou através de conexão com a rede Internet (TCP/IP) via rede WAN. Através do estudo de análise de vulnerabilidades nota-se vários pontos onde os atacantes externos e os internos podem obter acesso aos diversos equipamentos, tais como via rede de telefonia pública, rede corporativa, via rede sem fio, etc.

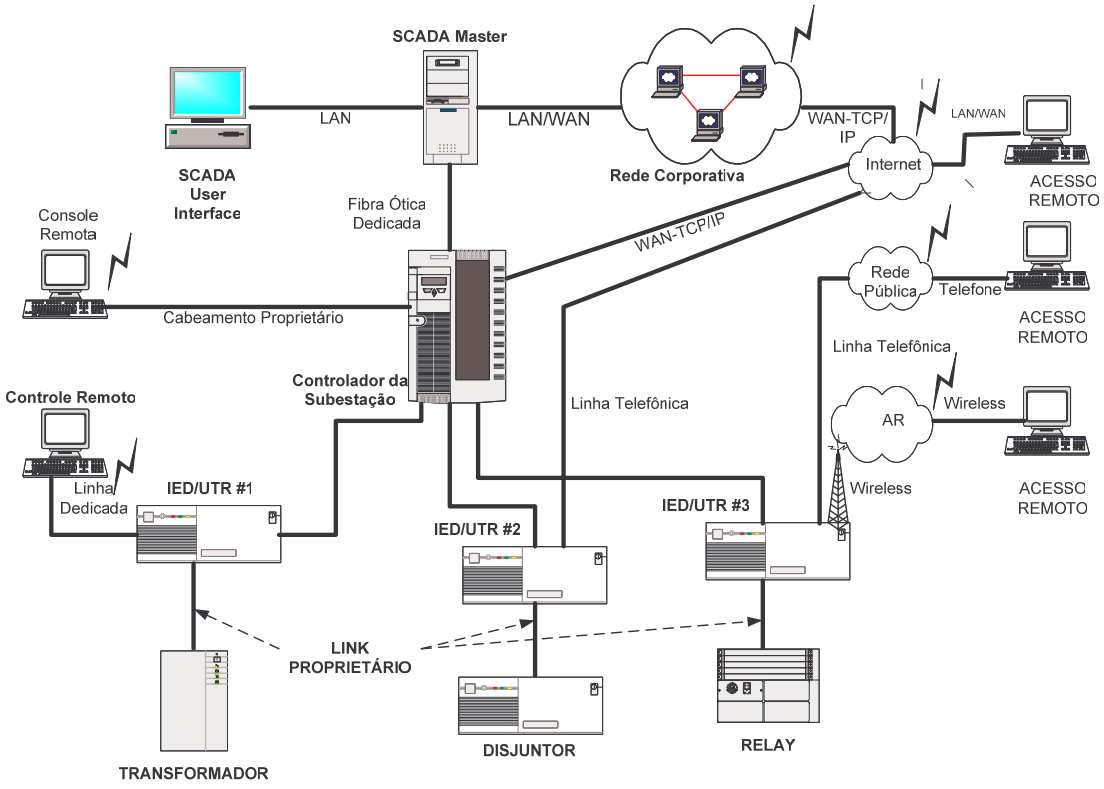


Figura 9.6 - Exemplo de um Sistema de Controle de Subestação.

Dos pontos apontados na figura 9.6, os atacantes (externos ou internos) podem ter acesso as UTRs ou IEDs e por conseguinte aos equipamentos e as medidas coletadas.

9.2 CENÁRIOS DE ATAQUES E A SOLUÇÃO PROPOSTA

Tomando como referência as Figuras 9.5 e 9.6, pode-se elaborar o seguinte cenário de ataque:

- Pela Figura 9.6, a IED/UTR # 2 pode ser considerada um potencial objeto de ataque em razão de sua conectividade com a Internet, que permite o acesso remoto, tanto diretamente via o controlador da subestação quanto via a rede corporativa.
- Caso o atacante (interno ou externo) consiga acesso a IED/UTR #2, duas prováveis situações podem ocorrer:
    - Atacante assume o controle sobre o disjuntor;
    - O atacante altera as informações da base de dados da UTR.

No primeiro caso o atacante poderia bloquear sinais de controle vindos do SCADA Master e enviar falsas confirmações. O operador poderia pensar que o disjuntor está fechado, mas ele está aberto, ou que ele está com problemas de funcionamento e ele não está. O atacante também poderia tomar controle direto do equipamento e enviar sinais de controle para desligá-lo. As tentativas do operador em religar o equipamento poderiam ser bloqueadas através de um ataque de negação de serviço.

No segundo caso o atacante poderia manipular as leituras de dados e corromper a base de dados do SCADA Master. Como mostra a figura 9.5, uma vez que ele invadisse a UTR #2 alterando o código DNP3 do usuário com algum tipo de "*exploit*", os dados coletados poderiam ser corrompidos e falsas informações seriam enviadas ao SCADA Master. Se o operador que estivesse no "*SCADA User Interface Console*" (veja

figura 9.6) tomar alguma ação baseada nestas informações corrompidas, toda a rede elétrica poderia vir a estar em perigo. Em suma a Base de Dados do SCADA Master não mais retrataria a realidade do Sistema Elétrico de Potência. Por exemplo, uma linha poderia indicar uma sobrecarga, o que levaria o operador a tomar medidas para desligá-la. Esta manobra, tomada em razão de uma informação falsa, poderia levar o sistema elétrico de potência como um todo a um colapso.

De tal forma a detectar estes cenários de ataque, é proposta a implementação de um detector de anomalias para identificar estas ameaças e informar através de um alarme a tentativa de ataque, bem como o tipo de ataque. Este modelo proposto deverá modelar o fluxo de dados normal e as operações de controle dentro do sistema SCADA através de técnicas inteligentes para detectar anomalias produzidas por mudanças nas informações coletadas do sistema elétrico de potência.

9.3 ARQUITETURA DO DETECTOR DE ANOMALIAS

A solução aqui proposta para o problema de detecção de anomalias presentes nos cenários de ataque descritos, utiliza técnicas inteligentes para extrair conhecimento do sistema SCADA. A abordagem aqui proposta divide-se em 2 etapas: Na primeira etapa o extrator de conhecimento deverá gerar um conjunto de regras que determinarão o comportamento normal ou anormal do sistema. Este conjunto de regras será definido através de informações coletadas "*offline*" do sistema SCADA, tais como medidas, estado das chaves ou disjuntores, tap, etc. e analisadas pelo especialista, para determinar sua normalidade ou não. Na segunda etapa, os dados oriundos das UTRs em tempo real passarão por este conjunto de regras, definindo assim a normalidade ou não das

informações coletadas. O diagrama da Figura 9.7 descreve o modelo proposto. Nesta etapa o detector de anomalias estabelecido pelas regras anteriormente extraídas deverá reconhecer a condição de anormalidade, podendo ainda proceder a algum tipo de classificação do tipo de ataque ocorrido. Por exemplo, considerando os cenários de ataque propostos no item 9.2, a condição de alarme da Figura 9.7 indicará se o estado do disjuntor foi alterado de forma maliciosa ou se a base de dados do SCADA Master foi corrompida.

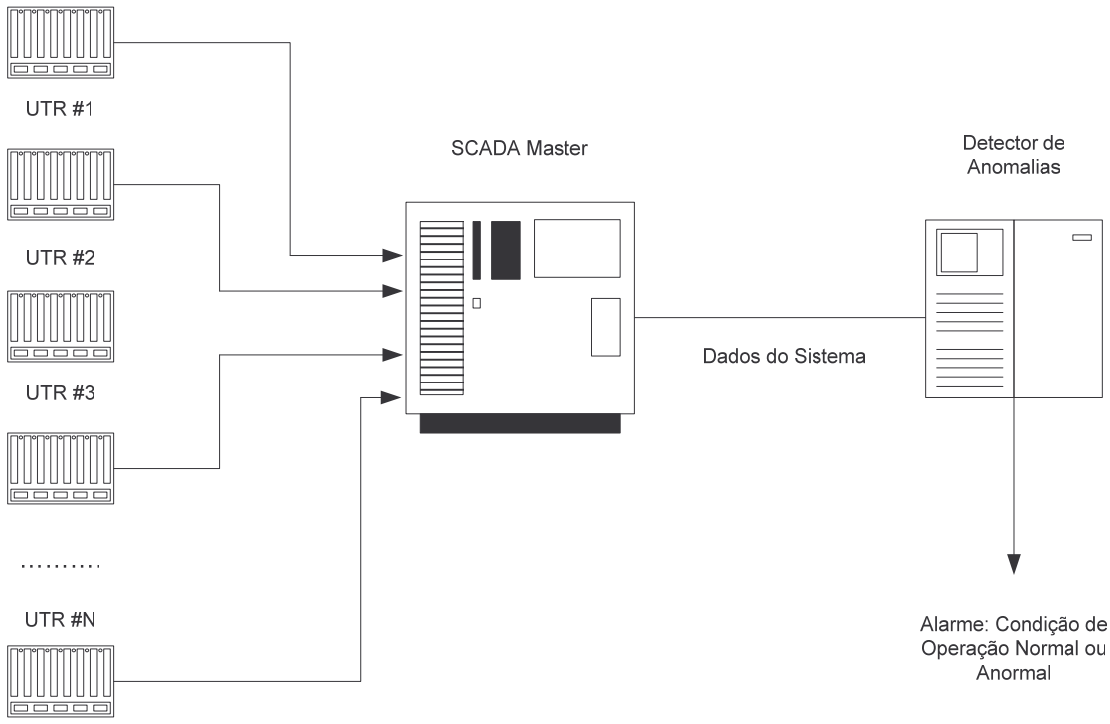


Figura 9.7 - Modelo do Detector de Anomalias.

9.4 IMPLEMENTAÇÃO DO DETECTOR DE ANOMALIAS

Em face ao grande volume de informações na base de dados do Servidor SCADA Master e a capacidade limitada dos recursos computacionais deste servidor, o

modelo de técnica inteligente recomendado deve reduzir o número de variáveis de entrada e o número de casos, oferecendo um conjunto de regras mais compacto para o detector de anomalias. O modelo proposto baseia-se na Teoria de Conjuntos Aproximados, proposto por Pawlak e descrito no item 8.3.

As principais vantagens do uso desta técnica são:

- Reduz o número de regras sem reduzir a base de conhecimento do sistema;
- Tem comportamento dinâmico, pois regras que não foram informadas pelo especialista podem ser extraídas do sistema.
- Reduz a necessidade de grandes recursos computacionais e de grande capacidade de memória;

A principal desvantagem está na necessidade do especialista para fornecer/classificar os dados do sistema e outras informações.

A seguir será apresentado um caso exemplo tomando por base a Figura 9.6 e os cenários de ataque apresentados no item 9.2. Considere a base de dados do centro de controle, representada pelo SCADA Master nas figura 9.5 e 9.6, composta por um conjunto de valores relativo às medidas coletadas da UTR/IED em estudo. Estes valores estão apresentados da Tabela 9.1. O estado operacional do sistema elétrico hipotético depende de 4 elementos: O status do disjuntor A, a capacidade de transmissão das linhas B e C e a tensão na barra D. Os atributos representados pelas colunas A, B, C, D da tabela 9.1 correspondem a:

- O estado do disjuntor A é definido por 0 (fechado) e 1(aberto);
- Os valores das linhas de transmissão B e C são porcentagens do fluxo de potência real de acordo com as suas capacidades máximas, em %;

- A tensão da barra D é expressa em PU;

A classificação de cada condição para o Estado Operacional do Sistema de Potência, S, é feita segundo o especialista em duas possíveis saídas: Normal (N) e Anormal (A). O nível anormal pode representar ações maliciosas na UTR/IED, segundo os cenários de ataque propostos no item 9.2.

Tabela 9.1 - Base de dados reduzida do SCADA Master.

	ATRIBUTOS				
U	**A**	**B**	**C**	**D**	**S**
1	0	57	82	1,07	A
2	0	37	32	0,97	A
3	1	0	87	0,95	A
4	1	72	31	1,07	A
5	0	28	39	1,02	A
6	0	42	82	1,07	A
7	0	52	59	1,01	N
8	1	62	67	1,04	A
9	0	57	45	0,99	N
10	0	45	58	1,00	N
11	0	32	57	0,94	N
12	0	0	57	1,08	A
13	1	58	87	1,03	A
14	0	58	56	1,07	A
15	0	25	57	1,03	N
16	0	56	54	1,08	A
17	1	59	72	1,08	A
18	0	32	0	0,93	A
19	0	32	45	0,94	N
20	1	72	67	0,96	A
21	0	57	45	1,01	N
22	0	32	45	0,94	N
23	0	29	43	1,08	A
24	1	0	72	0,95	A
25	1	57	79	1,07	A
26	0	31	43	0,99	N
27	0	32	42	0,94	N
28	0	17	32	0,92	A
29	0	23	22	1,00	A
30	0	23	57	0,91	N

O algoritmo que fornece as condições de redução é representado pelo diagrama na Figura 9.8.

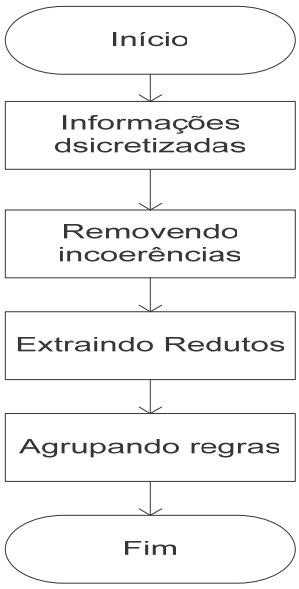


Figura 9.8 - Algoritmo para Extração de Conhecimento usando Teoria dos Conjuntos Aproximados.

Para o processo de discretização das informações (Primeiro Passo) considerou-se as seguintes faixas operacionais, para cada atributo:

- Atributo A: 0 e 1
- Atributo B e C:
    - Entre 0 e 40: L
    - Entre 40 e 60: M
    - Entre 60 e 100: H
- Atributo D:
    - Entre 0 e 0.95: L
    - Entre 0.95 e 1.05: N
    - Acima de 1.05: H

A Tabela 9.2 representa o passo final do processo de extração de conhecimentos. Pelo algoritmo da Figura 9.8, trata-se da tabela de extração de redutos. Esta tabela

representa o conjunto de regras que forma a base de conhecimento da tabela original. Esta base de conhecimento pode ser utilizada agora por um sistema especialista que irá analisar as informações na base de dados do SCADA Master e detectar se ocorreu ou não um ataque, provocado pela alteração de uma informação da base de dados do SCADA Master.

As regras especificadas para este caso com base na Tabela 9.2 são as seguintes:

IF C=H THEN SAIDA=A;
IF D=H THEN SAIDA=A;
IF C=L THEN SAIDA =A;
IF C=M AND D=N THEN SAIDA=N;
IF C=M AND D=L THEN SAIDA=N;

Tabela 9.2 - Redução do conjunto de exemplos.

Atributos				**Saída**
A	**B**	**C**	**D**	**S**
-	**-**	**H**	**-**	**A**
-	**-**	**-**	**H**	**A**
-	**-**	**L**	**-**	**A**
-	**-**	**M**	**N**	**N**
-	**-**	**M**	**L**	**N**

O Anexo A mostra os resultados da simulação destas regras para o conjunto de dados especificados na Tabela 9.1 e com um conjunto de dados corrompido. Nota-se que os valores para a saída S da Tabela 9.1 são mantidos quando utilizamos a base de dados original.

Na segunda etapa, a Tabela 9.1 é transformada na Tabela 9.3. Nesta tabela foram especificadas 3 possibilidades para cada condição anormal: Nível 1 (EN1), Nível 2 (EN2) e Nível 3 (EN3). Caso contrário especifica-se a condição Normal (N). Novamente utiliza-se um especialista para definir o estado operacional S do sistema elétrico para cada exemplo da tabela. A Tabela 9.4 representa o passo final do processo de extração de conhecimentos.

Tabela 9.3 - Nova base de dados com 3 níveis para condição anormal

	ATRIBUTOS				
U	**A**	**B**	**C**	**D**	**S**
1	0	57	82	1,07	EN2
2	0	37	32	0,97	EN1
3	1	0	87	0,95	EN3
4	1	72	31	1,07	EN3
5	0	28	39	1,02	EN1
6	0	42	82	1,07	EN2
7	0	52	59	1,01	N
8	1	62	67	1,04	EN3
9	0	57	45	0,99	N
10	0	45	58	1,00	N
11	0	32	57	0,94	N
12	0	0	57	1,08	EN2
13	1	58	87	1,03	EN3
14	0	58	56	1,07	EN2
15	0	25	57	1,03	N
16	0	56	54	1,08	EN2
17	1	59	72	1,08	EN3
18	0	32	0	0,93	EN1
19	0	32	45	0,94	N
20	1	72	67	0,96	EN3
21	0	57	45	1,01	N
22	0	32	45	0,94	N
23	0	29	43	1,08	EN2
24	1	0	72	0,95	EN3
25	1	57	79	1,07	EN3
26	0	31	43	0,99	N
27	0	32	42	0,94	N
28	0	17	32	0,92	EN1
29	0	23	22	1,00	EN1
30	0	23	57	0,91	N

As regras especificadas para este caso com base na Tabela 9.4 são as seguintes:

IF A=0 AND C=H THEN SAIDA=EN2;

IF A=0 AND D=H THEN SAIDA=EN2;

IF A=0 AND C=L THEN SAIDA=EN1;

IF C=L AND D=N THEN SAIDA=EN1;

IF A=1 THEN SAIDA=EN3;
IF C=H AND D=N THEN SAIDA=EN3;
IF C=L AND D=H THEN SAIDA=EN3;
IF C=M AND D=N THEN SAIDA=N;
IF C=M AND D=L THEN SAIDA=N;
IF C=M AND D=H THEN SAIDA=EN2;
IF C=L AND D=L THEN SAIDA=EN1.

Tabela 9.4 - Redução do conjunto de exemplos

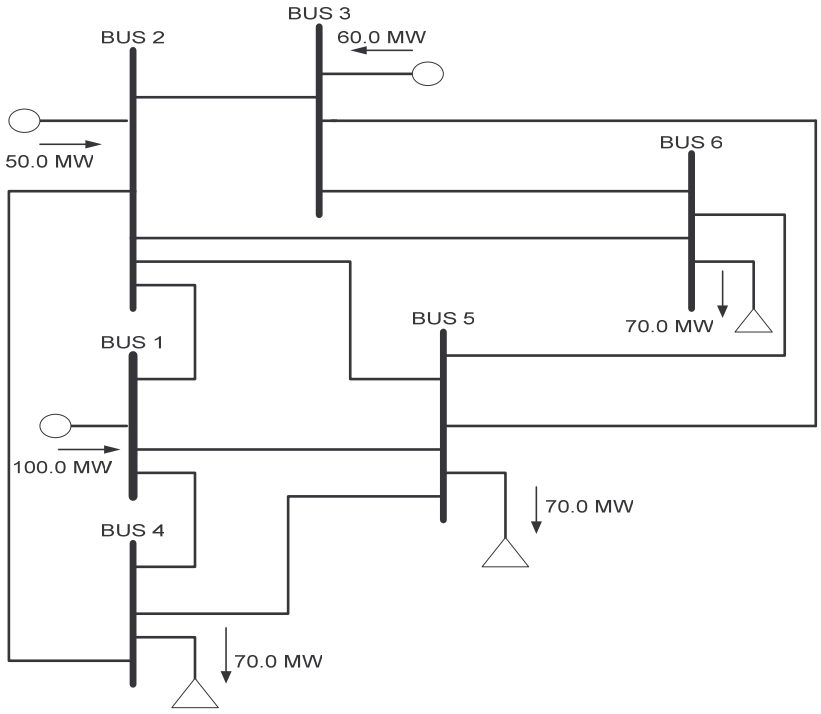
ATRIBUTOS				**SAIDA**
A	**B**	**C**	**D**	**S**
0	-	H	-	EN2
0	-	-	H	EN2
0	-	L	-	EN1
-	-	L	N	EN1
1	-	-	-	EN3
-	-	H	N	EN3
-	-	L	H	EN3
-	-	M	N	N
-	-	M	L	N
-	-	M	H	EN2
-	-	L	L	EN1

Este conjunto de regras forma a base de conhecimentos a ser utilizada pelo detector de anomalias. Tanto o caso 1 quanto o caso 2, apresentam um conjunto mínimo de regras ressaltando uma das características da teoria dos conjuntos aproximados que é a redução dos exemplos e consequentemente da base de conhecimento sem a perda de informação original.

9.5 CASO TESTE SISTEMA ELÉTRICO DE POTÊNCIA DE 6 BARRAS

Para a seqüência de testes a seguir será utilizado o modelo de sistema elétrico de potência descrito em [140]. Trata-se de um sistema de 6 barras, conforme pode ser visualizado no diagrama unifilar da fig. 9.9. Serão elaborados casos testes que deverão

validar a proposição de detecção de anomalias produzidas por erros introduzidos no Sistema SCADA através de ações maliciosas. Ao final será apresentado o conjunto de resultados dos testes realizados e uma análise das respostas obtidas. Pretende-se demonstrar a validade da metodologia empregada pelo Sistema de Detecção de Anomalias proposto usando a Teoria dos Conjuntos Aproximados para, em conjunto com o Programa de Estimação de Estado, melhorar a confiabilidade e proteção de Sistemas Elétricos de Potência, como Infra-estrutura Crítica, em face a novas ameaças provenientes de ataques cibernéticos.



Fiura .9.9-Sistema Elétrico de Potência de 6 Barras [140]

9.5.1 Metodologia

Neste novo caso, criou-se um ambiente de testes contendo alguns componentes chaves presentes em um centro de controle: Fluxo de Carga, Sistema SCADA e o

Estimador de Estados. Além disso, é implementado o Módulo Extrator de Regras baseado na Teoria dos Conjuntos Aproximados e o Detector de Anomalias usando as regras extraídas. A arquitetura deste ambiente de testes está apresentada na fig. 9.10. A seguir, é descrito os componentes utilizados.

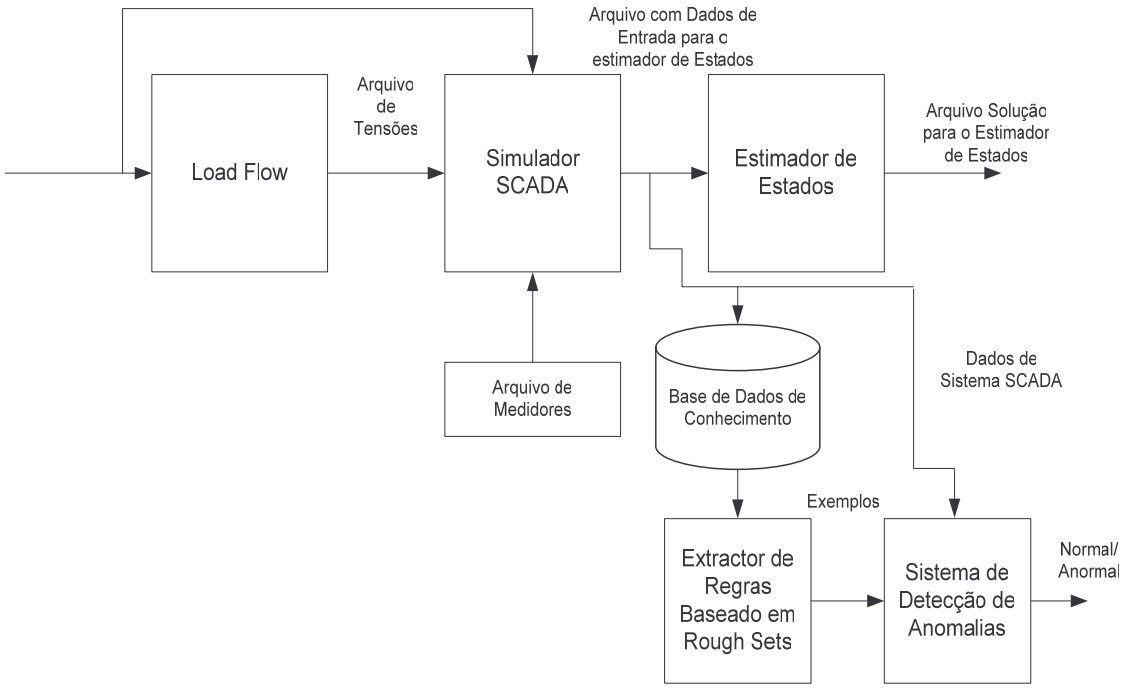


Figura 9.10-Ambiente de Testes para o Detector de Anomalias Proposto

- **Módulo para Cálculo do Fluxo de Carga (Load Flow):** É o módulo utilizado para calcular o fluxo de potência de um sistema elétrico de potência. Ele foi adaptado de [140].
- **Módulo Simulador SCADA:** Este módulo simula as funções realizadas pelo sistema de aquisição de dados e controle supervisório online (SCADA). A idéia é simular a rede elétrica, calcular as tensões, fluxo de potência e cargas no sistema e então associá-las com os medidores previamente especificados em um arquivo de configuração. Ele foi adaptado de [140].

- **Módulo Estimador de Estados:** Módulo adaptado de [140] e usado para realizar o processo de estimação de estados.
- **Módulo Extrator de Regras:** Módulo utilizado para extrair regras da base de conhecimentos, usando o Algoritmo de Classificação por Conjuntos Aproximados;
- **Módulo para Detecção de Anomalias:** Este módulo usa as regras definidas pelo Módulo de Extração de Regras para determinar o estado dos dados do sistema oriundos do Sistema SCADA.

Para que o Sistema Elétrico de Potência possa operar corretamente é necessário que os dados de tensão, freqüência e fluxo de potência coletados pelo Sistema SCADA sejam mantidos dentro de faixas e limites de segurança. O processo de Estimação de Estados consiste na obtenção em tempo real destas grandezas [141]. De acordo com [140], Estimação de Estado atribui um valor a uma variável de estado desconhecida baseada nas medidas obtidas daquele sistema de acordo com certo critério. Segundo [125], "algorítmos para estimação de estados reconstroem o estado do sistema de potência no caso da perda e/ou corrupção do dado. Este modelo, entretanto, não aborda o problema de fornecer a avaliação do estado normal ou anormal do sistema, e, em alguns casos poderia esconder indícios de um ataque ou de outras anomalias". Esta é uma suposição de risco, visto que em geral ocorrem erros de configuração, e há sempre a possibilidade de um atacante estar entre o centro de controle e o sistema elétrico.

9.5.2 Estudo de Caso 1: Corrompendo os Valores de Potência

Para testar o modelo de detecção de anomalia proposto foi usado o ambiente de testes apresentado na fig. 9.10 e o sistema elétrico de seis barras descrito em [140] e

apresentado na fig. 9.9. Os dados de teste foram gerados através da corrupção dos valores produzidos pelo módulo Simulador SCADA. Segundo [142] o processo de estimação de estado está sujeito a três tipos de erros: erros nas medidas analógicas (erros grosseiros); erros devido a informações erradas quanto aos estados de chaves e/ou disjuntores (erros topológicos) e erros causados por informações erradas de algum parâmetro do sistema (erros de parâmetros). Já Xuan Jin et al [143], considera a possibilidade de existência de 5 tipos de erros aplicados aos dados provenientes de sistemas elétricos: "bias" constante com desvios distribuídos normalmente, perda do ponto decimal (mantissa), troca de sinal, valor fixo por um período de tempo fixo e valor aleatório por um período de tempo fixo. Os autores atribuem estes erros ao fato de que medidas elétricas podem ser alteradas devido a ruído, ataques, erros de software, falha de medidores, EMI e erros de transmissão.

A capacidade do modelo de detecção de anomalia proposto para identificar condições normais e anormais será avaliada em relação à capacidade do módulo de estimação de estados de fornecer um resultado razoável, mesmo considerando que os dados tenham sido corrompidos de alguma forma.

No caso em estudo, o Módulo Simulador SCADA utiliza um conjunto de 29 medidores representados na figura 9.11. A localização e o tipo do medidor (Tensão ou Potência) são especificados no arquivo de medidores do Módulo Simulador SCADA, como indicado na fig. 9.10. Como apresentado nas figuras 9.5 e 9.6, num ambiente real estes medidores são conectados a UTRs que enviam os dados coletados para o Centro de Controle, onde o operador analisa os resultados produzidos pelo Módulo de

Estimação de Estados em função dos dados coletados e toma as ações necessárias para manter as condições operacionais do Sistema.

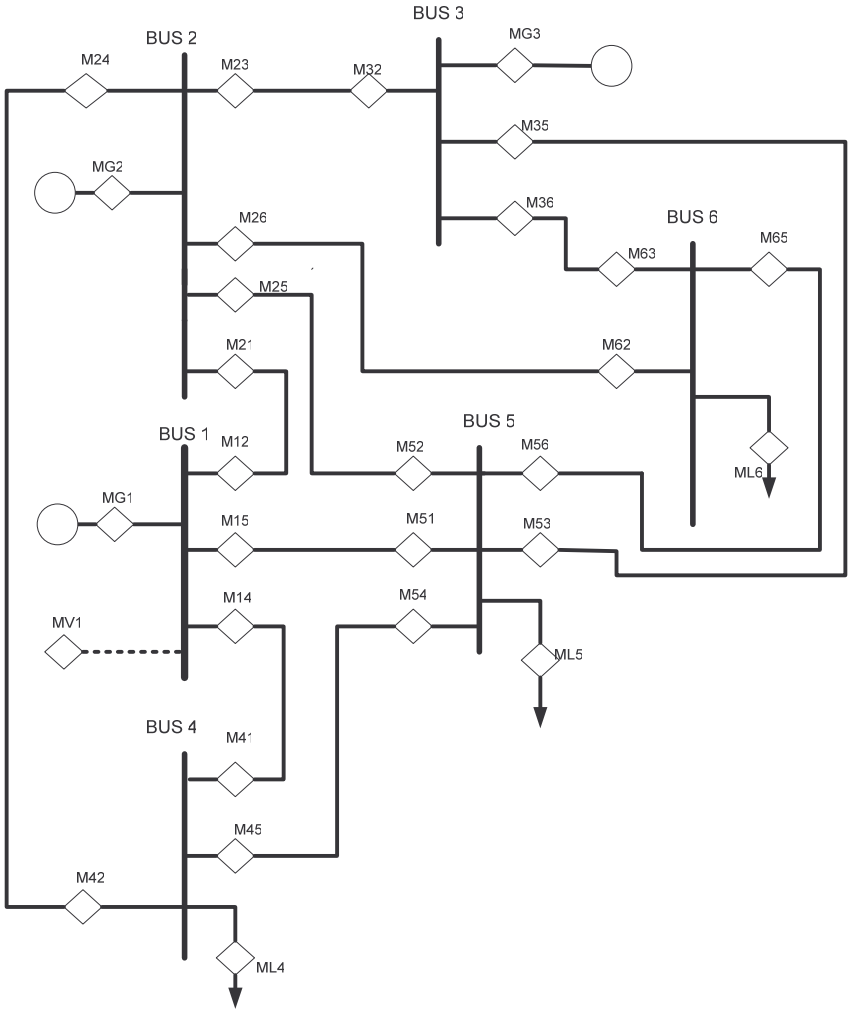


Figura 9.11- Sistema de 6 barras com medidores

Para montar a base de conhecimentos do primeiro caso teste gerou-se, inicialmente, 25 exemplos, através da variação do valor da carga nas barras 4 e 6. A faixa de variação dos valores de potência ativa em valor absoluto foi de **0.5 pu <= Potência Ativa <= 0.9 pu**, em intervalos de 0.05 pu. Em nosso ambiente de testes, representado na figura 9.10, estes exemplos são montados pelo módulo Simulador SCADA. Cada exemplo consta de 57 valores, sendo que cada um deles refere-se a uma medida realizada pelos medidores especificados no arquivo de configuração de

medidores. Desta forma a base de conhecimentos gerada totaliza 64 exemplos, dos quais 39 exemplos foram gerados a partir da corrupção do sinal nos valores de potência ativa. Para facilitar a análise preliminar deste primeiro caso teste, os erros foram aplicados somente nas barras 4 e 6 do sistema de 6 barras. O tipo de erro introduzido envolveu somente a inversão do sinal dos valores de potência ativa no arquivo de saída do Módulo Simulador SCADA, como mostrado no trecho de listagem a seguir. Os valores apontados eram inicialmente **-8.9991317636E-01 e -6.9994161078E-01.**

```
SIXBUS POWER FLOW SAMPLE SYSTEM
-------------------------------
6
11
LINE    1    2  1.00000E-01  2.00000E-01  2.00000E-02
LINE    1    4  5.00000E-02  2.00000E-01  2.00000E-02
LINE    1    5  8.00000E-02  3.00000E-01  3.00000E-02
LINE    2    3  5.00000E-02  2.50000E-01  3.00000E-02
LINE    2    4  5.00000E-02  1.00000E-01  1.00000E-02
LINE    2    5  1.00000E-01  3.00000E-01  2.00000E-02
LINE    2    6  7.00000E-02  2.00000E-01  2.50000E-02
LINE    3    5  1.20000E-01  2.60000E-01  2.50000E-02
LINE    3    6  2.00000E-02  1.00000E-01  1.00000E-02
LINE    4    5  2.00000E-01  4.00000E-01  4.00000E-02
LINE    5    6  1.00000E-01  3.00000E-01  3.00000E-02
V    1     1.0500000000E+00  1.000E-04
A    1     0.0000000000E+00  1.000E-04
I    1     1.2926382831E+00  1.000E-02     2.5547635626E-01  1.000E-02
I    2     4.9990173678E-01  1.000E-02     1.0004148677E+00  1.000E-02
I    3     5.9995430599E-01  1.000E-02     5.9999305592E-01  1.000E-02
I    4    +8.9991317636E-01  1.000E-02    -7.0000930338E-01  1.000E-02
I    5    -6.9994125684E-01  1.000E-02    -6.9999348948E-01  1.000E-02
I    6    +6.9994161078E-01  1.000E-02    -6.9998235508E-01  1.000E-02
F    1     2      3.5417726409E-01  1.000E-02    -1.5040670241E-01  1.000E-02
F    1     4      5.4460436822E-01  1.000E-02     2.4278040036E-01  1.000E-02
F    1     5      3.9385665081E-01  1.000E-02     1.6310265830E-01  1.000E-02
F    2     1     -3.4130497589E-01  1.000E-02     1.3231241138E-01  1.000E-02
F    2     3      1.2609734643E-02  1.000E-02    -6.7821822666E-03  1.000E-02
F    2     4      4.1365251965E-01  1.000E-02     4.7143716966E-01  1.000E-02
F    2     5      1.5270749550E-01  1.000E-02     1.8889744167E-01  1.000E-02
F    2     6      2.6223696287E-01  1.000E-02     2.1455002730E-01  1.000E-02
F    3     2     -1.2571647608E-02  1.000E-02    -5.7969124298E-02  1.000E-02
```

Erros introduzidos aqui: Inversão de de sinal – por +

Examinando o arquivo, nota-se que além do valor de potência ativa e reativa, indicado pela letra I, também existe a possibilidade de alterar os valores de tensão (indicado pela letra V e A) e do fluxo de potência ativa e reativa nas linhas, indicado pela letra F.

A Base de Conhecimento foi estabelecida por 64 exemplos, cada exemplo com 57 valores. Isto fornece um total de 64*57=3,648 valores. Como mostrado no ambiente

de teste da figura 9.10, estes 64 exemplos foram tratados pelo Módulo de Extração de Regras gerando, então, as seguintes regras:

- **If (Potência Ativa na Barra 4 >=-0.62)&(Potência Ativa na Barra 4 <-0.3)&(Potência Ativa na Barra 6 >=-0.9)&(Potência Ativa na Barra 6 <-0.6) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.9)&(Potência Ativa na Barra 4 <-0.6)&(Potência Ativa na Barra 6 >=-0.6)&(Potência Ativa na Barra 6 < -0.3) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.6)&(Potência Ativa na Barra 4 < -0.3)&(Potência Ativa na Barra 6 >=-0.6)&(Potência Ativa na Barra 6 < -0.6) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.9)&(Potência Ativa na Barra 4 < -0.6)&(Potência Ativa na Barra 6 >=-0.9)&(Potência Ativa na Barra 6 <-0.6) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >= 0.3)&(Potência Ativa na Barra 4 < 0.6) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 6 >=0.6)&(Potência Ativa na Barra 6 < 0.95) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 6 >= 0.3)&(Potência Ativa na Barra 6 < 0.6) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 4 >= 0.6)&(Potência Ativa na Barra 4 < 0.95) then (RESULTADO = ANORMAL)**

Estas regras mostram bem como foi a redução dos dados: o Módulo Extrator de Regras extraiu 8 regras de um total de 3648 amostras.

Todos os 64 exemplos contidos na Base de Conhecimento foram testados com o Módulo de Detecção de Anomalias implementado em Matlab usando as regras acima

enumeradas. O Código-fonte em Matlab para implementar este módulo está apresentado no Anexo C.1

A fim de avaliar o conjunto de regras gerado pelo extrator para implementar o detector de anomalias, foi criado um caso teste com 20 exemplos e submetido ao mesmo módulo de detecção de anomalias. Os erros introduzidos no arquivo gerado pelo módulo são todos do tipo troca de sinal. Este arquivo é apresentado no Anexo C.2. O resultado do processamento deste arquivo pelo módulo Detector de Anomalias é apresentado no Anexo C.3.

A Tabela 9.5 apresenta a comparação dos resultados obtidos pelo Detector de Anomalias e o Módulo de Estimação de Estados. Os valores IMW4 e IMW6 correspondem ao valor da carga nas barras 4 e 6, respectivamente. Os fluxos nas linhas 4-1, 4-2, 4-5, 6-2, 6-3 e 6-5 foram obtidos pelo Módulo de Estimação de Estados. Cada grupo de 2 exemplos apresenta uma entrada normal e uma entrada corrompida através da alteração do sinal, conforme arquivo apresentado no Anexo C.2. A saída do detector de anomalias apresenta 3 possíveis estados: Normal, Anormal e Fora de Faixa. O último estado sinaliza valores fora da faixa para os exemplos gerados na base de conhecimento. Desta forma os valores -0.45 pu para IMW4 e -0.95 pu para IMW6 estão fora da faixa especificada inicialmente em abs(0.5 pu) <= Potência Ativa <=abs(0.9 pu). Desta forma, é muito importante a geração correta dos exemplos que compõem a base de conhecimentos, para que erros deste tipo não ocorram. Este é um exemplo somente para demonstração da validade da proposta. Em casos reais a base de conhecimento é extremamente grande e produz poucas variações.

Tabela 9.5 - Resumo dos resultados do Caso 1obtidos pelo Detector de Anomalias e o Módulo Estimador de Estados

IMW4 Pu	IMW6 pu	LINHA 4 TO 1 MW	LINHA 4 TO 2 MW	LINHA 4 TO 5 MW	LINHA 6 TO 2 MW	LINHA 6 TO 3 MW	LINHA 6 TO 5 MW	STATUS DETETOR DE ANOMALIAS	TIPO DE ERRO INTRODUZIDO
-0.63	-0.73	-39.83	-28.75	5.58	-27.17	-43.82	-2.02	Normal	Sem erro
+0.63	-0.73	-21.41	2.92	15.91	-33.59	-43.58	-2.54	Anormal	Troca de sinal
-0.53	-0.83	-37.75	-22.69	7.44	-31.44	-47.32	-4.24	Normal	Sem erro
-0.53	+0.83	-36.69	-31.06	5.85	-4.3	-10.45	13.77	Anormal	Troca de sinal
-0.77	-0.61	-43.38	-36.76	3.13	-22	-39.62	0.62	Normal	Sem erro
0.77	+0.61	-20.03	-4.36	14.59	-10	-12.8	13.28	Anormal	Troca de sinal
-0.71	-0.52	-37.46	-36.69	3.15	-18.47	-36.45	2.92	Normal	Sem erro
-0.71	+0.52	-36.8	-41.9	2.14	-1.37	-13.35	14.26	Anormal	Troca de sinal
-0.45	-0.95	-37.32	-16.9	9.23	-36.48	-51.54	-6.98	Fora de faixa	Sem erro
+0.45	-0.95	-24.17	5.8	16.63	-41.03	-51.38	-7.36	Anormal	Troca de sinal
-0.83	-0.78	-51.62	-35.05	3.69	-28.8	-45.61	-3.57	Normal	Sem erro
-0.83	+0.78	-50.68	-42.91	2.18	-3.27	-10.97	13.34	Anormal	Troca de sinal
-0.56	-0.88	-40.82	-22.65	7.47	-33.41	-49.09	-5.49	Normal	Sem erro
0.56	+0.88	-23.29	-3.39	15.01	-10.54	-9.75	13.14	Anormal	Troca de sinal
-0.56	-0.56	-30.87	-30.25	5.11	-20.41	-37.84	2.25	Normal	Sem erro
+0.56	-0.56	-14.3	-2.24	14.26	-26.12	-37.62	1.79	Anormal	Troca de sinal
-0.6699	-0.8599	-45.85	-27.22	6.18	-32.38	-48.4	-5.21	Normal	Sem erro
-0.6699	+0.8599	-44.79	-35.89	4.43	-4.29	-10.21	13.43	Anormal	Troca de sinal
-0.601	-0.7661	-39.4	-26.82	6.17	-28.69	-45.88	-2.83	Normal	Sem erro
-0.601	+0.7661	-38.48	-34.54	4.7	-3.61	-11.05	13.8	Anormal	Troca de sinal

O gráfico da Figura 9.12 apresenta uma comparação dos valores obtidos através do Módulo de Estimação de Estados para os dois primeiros exemplos da Tabela 9.5. Neste caso o valor da carga na barra 4 foi invertido (de -0.63 para +0.63), significando uma alteração no dado originalmente gerado pelo Módulo Load Flow e pelo Módulo Simulador SCADA. Esta alteração significa que os valores que foram entregues ao estimador de estados foram corrompidos.

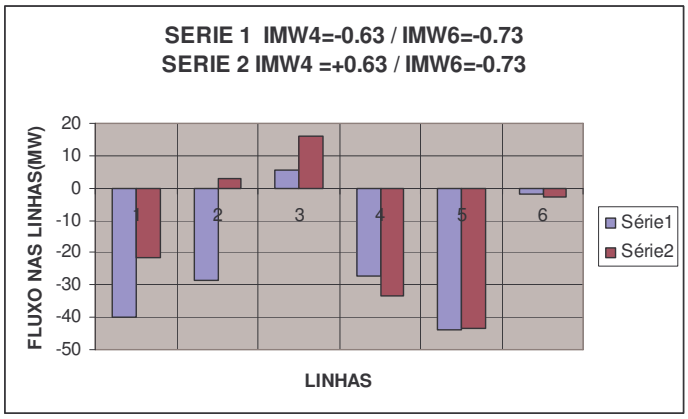


Figura 9.12-Caso 1 IMW4=-0.63 e IMW6=-0.73

Observando o gráfico da Figura 9.12 conclui-se que os valores do fluxo de potência para as linhas 6-2, 6-3 e 6-5 ficaram praticamente inalterados, mesmo na presença de erros. Contudo as linhas 4-1, 4-2 e 4-5 apresentaram valores discrepantes com relação ao valor original. Se, por exemplo, a capacidade nominal das linhas 4-1, 4-2 e 4-5 for, respectivamente, 50 MW, 40 MW e 10 MW, a linha 4-5 estaria cerca de 60% além de sua capacidade nominal (isto é, 15.91/10=1.59). Caso o operador considerasse estes resultados, isto o levaria a pensar em uma sobrecarga na capacidade da linha 4-5. Neste caso ele poderia adotar medidas para sanar o "falso problema", pondo em risco a estabilidade do sistema. Diferentemente, o Detector de Anomalias classificou este exemplo como Anormal, apontando para uma possível corrupção dos valores lidos do sistema SCADA.

Outro exemplo pode ser visto no gráfico da Figura 9.13. Neste caso as linhas 4-1, 4-2 e 4-5 apresentaram valores compatíveis entre o caso original e o caso corrompido. Já as linhas 6-2, 6-3 e 6-5 apresentaram valores discrepantes entre o caso original e o caso corrompido.

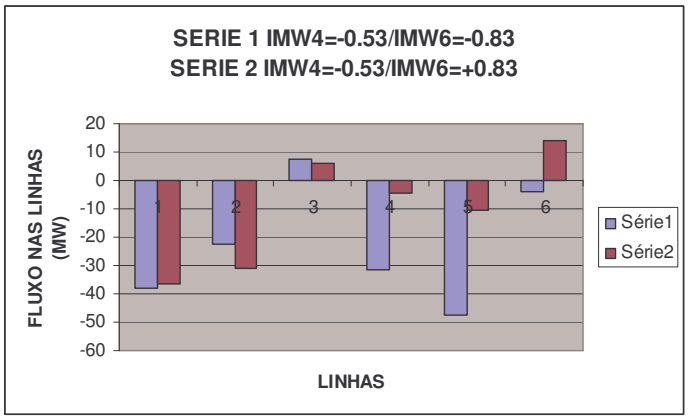


Figura 9.13-Caso IMW4=-0.53 e IMW6=-0.83

Da mesma forma, se a capacidade nominal das linhas 6-2, 6-3 e 6-5 for considerada 50 MW, 40 MW e 10 MW, respectivamente, o valor apresentado pela linha 6-5 estaria cerca de 37 % além da capacidade nominal (isto é, 13.37/10=1,37). Este fato poderia levar a uma operação errada por parte do operador, caso ele se baseasse nos valores apresentados pelo Módulo de Estimação de Estados. Já o Módulo de Detecção de Anomalias detectou que este exemplo apresenta uma condição anormal, indicando que houve alguma forma de corrupção de valores.

Os outros casos podem ser visualizados nos gráficos apresentados nas figuras a seguir (9.14 até 9.17). Em todos eles nota-se a ocorrência de valores discrepantes apresentados pelo Módulo de Estimação de Estados oriundos da mudança de sinal de 1 valor ou de 2 valores da potência ativa da carga na barra 4 e na barra 6. Como esperado, em todos os casos em que este tipo de ocorrência aconteceu, o Módulo Detector de Anomalias indicou a condição de anormalidade nos valores apresentados.

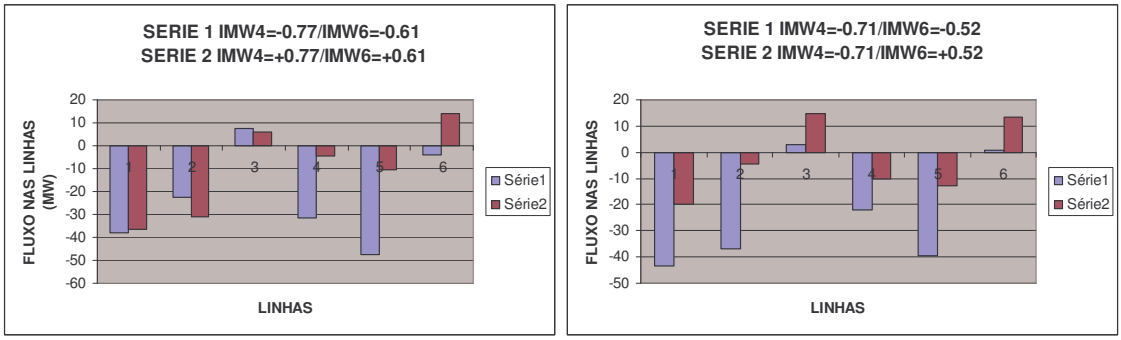


Figura 9.14-Comparando Caso Original e Caso Corrompido

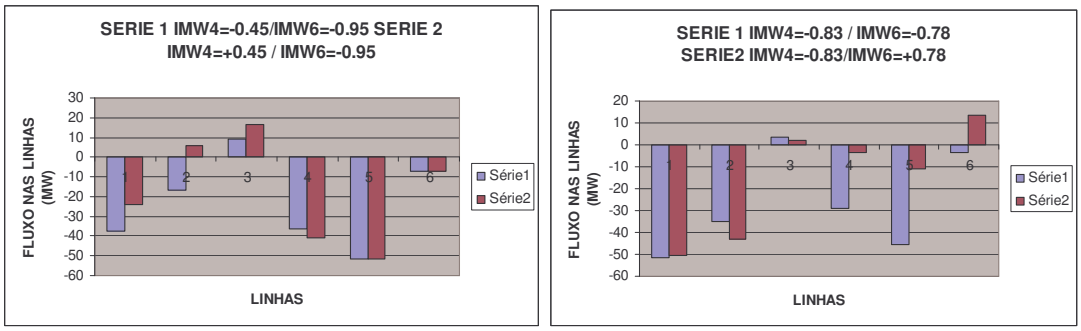


Figura 9.15-Comparando Caso Original e Caso Corrompido

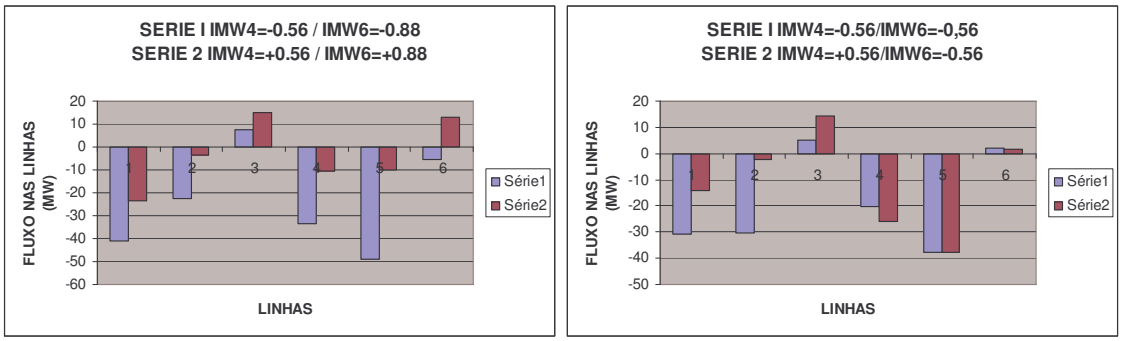


Figura 9.16-Comparando Caso Original e Caso Corrompido

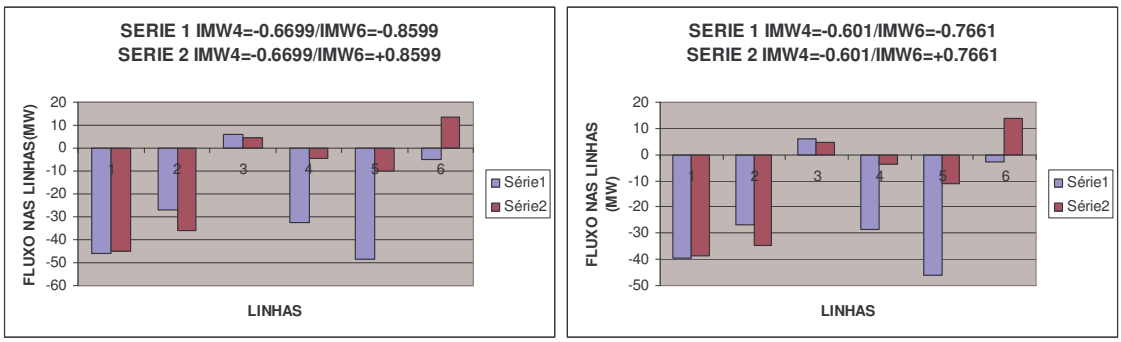


Figura 9.17-Comparando Caso Original e Caso Corrompido

9.5.3 Estudo de Caso 2: Ampliando a Faixa Operacional

Para ampliar os estudos sobre a validade das regras definidas pelo módulo de extração de regras, foi criado um segundo caso teste, expandindo as faixas operacionais para os valores de potência ativa nas barras 4 e 6. O novo arquivo de exemplos possui 162 exemplos com valores variando de 0.3 pu a 1.10 pu em intervalos de 0.05 pu. O erro introduzido no arquivo de saída do Módulo Simulador SCADA envolveu novamente a troca de sinal. A Base de Conhecimento gerada para este novo caso contém 162 exemplos cada um dos quais com 57 medidas, definidas pelos medidores estabelecidos pelo Arquivo de Medidores utilizado pelo Módulo Simulador SCADA (Fig. 9.11). Os exemplos considerados como operação normal foram classificados como NORMAL e aqueles que apresentaram corrupção do sinal foram classificados como ANORMAL. A Base de Conhecimento assim estabelecida foi tratada pelo Módulo de Extração de Regras, que gerou as seguintes regras:

- **If (Potência Ativa na Barra 4 >=-0.7333) & (Potência Ativa na Barra 4 < -0.3667) & (Potência Ativa na Barra 6 >=-0.7333) & (Potência Ativa na Barra 6 <-0.-0.3667)then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-1.1) & (Potência Ativa na Barra 4 < -0.7333)&(Potência Ativa na Barra 6 >=-0.7333)&(Potência Ativa na Barra 6 < -0.3667) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.7333) & (Potência Ativa na Barra 4 < -0.3667) & (Potência Ativa na Barra 6 >=-1.1) & (Potência Ativa na Barra 6 < -0.7333) then (RESULTADO=NORMAL)**

- **If (Potência Ativa na Barra 4 >=-1.1) & (Potência Ativa na Barra 4 < -0.7333) & (Potência Ativa na Barra 6 >=-1.1) & (Potência Ativa na Barra 6 <-0.7333) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >= 0.3667) & (Potência Ativa na Barra 4 < 07333) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 6 >=0.3667) & (Potência Ativa na Barra 6 < 1.101) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 4 >= 0.7333) & (Potência Ativa na Barra 4 < 1.101) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 6 >= 0.7333) & (Potência Ativa na Barra 6 < 1.101) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.3667) & (Potência Ativa na Barra 4 < 0.0) & (Potência Ativa na Barra 6>=-0.7333) & (Potência Ativa na Barra6<-0.3667) then (RESULTADO = NORMAL) & (Potência Ativa na Barra 4 < -0.3667) & (Potência Ativa na Barra 6>=-03667) & (Potência Ativa na Barra 6 < 0.0) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.3667) & (Potência Ativa na Barra 4 < 0.0) & (Potência Ativa na Barra 6>= -0.3667) & (Potência Ativa na Barra 6 <0.0) then (RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >= 0.0) & (Potência Ativa na Barra 4 < 0.3667) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 6 >= 0.0) & (Potência Ativa na Barra 6 < 0.3667) then (RESULTADO = ANORMAL)**

- **If (Potência Ativa na Barra 4 >=-0.3667) & (Potência Ativa na Barra 4 < 0.0) & (Potência Ativa na Barra 6 >=-1.1) & (Potência Ativa na Barra 6 <-0.7333) then(RESULTADO = NORMAL)**

- **If (Potência Ativa na Barra 4 >=-1.1) & (Potência Ativa na Barra 4 <-0.7333) & (Potência Ativa na Barra 6 >= -0.3667) & (Potência Ativa na Barra 6 < 0.0) then (RESULTADO = NORMAL)**

Desta forma gerou-se um conjunto de 15 regras a partir dos 162 exemplos presentes na Base de Conhecimento. Estas regras mostram a proporção da redução dos dados: o Módulo Extrator de Regras extraiu 15 regras simples de um total de 9234 amostras.

O Módulo de Detecção de Anomalias implementado em Matlab usando as regras acima descritas está apresentado no Anexo D.1. Usando o mesmo arquivo de exemplos do caso anterior com este novo conjunto regras, obtém-se a seguinte saída:

```
» regrasdb
Entre com nome do arquivo de dados: 'caso_teste.txt'
Entre com número de entradas: 20
Entrada:   -0.630   -0.730   Resultado: NORMAL
Entrada:   -0.530   -0.830   Resultado: NORMAL
Entrada:   -0.770   -0.610   Resultado: NORMAL
Entrada:   -0.710   -0.520   Resultado: NORMAL
Entrada:   -0.450   -0.950   Resultado: NORMAL
Entrada:   -0.830   -0.780   Resultado: NORMAL
Entrada:   -0.560   -0.880   Resultado: NORMAL
Entrada:   -0.560   -0.560   Resultado: NORMAL
Entrada:   -0.670   -0.860   Resultado: NORMAL
Entrada:   -0.601   -0.766   Resultado: NORMAL
Entrada:   +0.630   -0.730   Resultado: ANORMAL
Entrada:   -0.530   +0.830   Resultado: ANORMAL
Entrada:   +0.770   +0.610   Resultado: ANORMAL
Entrada:   -0.710   +0.520   Resultado: ANORMAL
Entrada:   +0.450   -0.950   Resultado: ANORMAL
Entrada:   -0.830   +0.780   Resultado: ANORMAL
Entrada:   +0.560   +0.880   Resultado: ANORMAL
Entrada:   +0.560   -0.560   Resultado: ANORMAL
Entrada:   -0.670   +0.860   Resultado: ANORMAL
Entrada:   -0.601   +0.766   Resultado: ANORMAL
```

Observa-se que o Módulo de Detecção de Anomalias realizou a detecção correta dos exemplos em que o sinal foi corrompido. Com a ampliação da faixa operacional dos exemplos da Base de Conhecimento, o caso classificado “FORA DE FAIXA” no primeiro caso agora foi corretamente classificado como um exemplo normal.

Um novo conjunto de testes foi criado para este modelo de detecção de anomalias contendo 20 exemplos como apresentado a seguir. Nesta saída foi ressaltada a troca de sinais de 1 medida e de 2 medidas. Estas medidas correspondem aos valores da potência ativa na Barra 4 (IMW4) e potência ativa na barra 6 (IMW6).

```
» regrasdb
Entre com nome do arquivo de dados: 'caso5.txt'
Entre com número de entradas: 20
             IMW4     IMW6
Entrada:   -0.310   -0.700   Resultado: NORMAL
Entrada:   +0.310   -0.700   Resultado: ANORMAL
Entrada:   -0.700   -0.430   Resultado: NORMAL
Entrada:   -0.700   +0.430   Resultado: ANORMAL
```

```
Entrada:   -0.480   -0.423   Resultado: NORMAL
Entrada:   +0.480   +0.423   Resultado: ANORMAL
Entrada:   -0.980   -0.610   Resultado: NORMAL
Entrada:   -0.980   +0.610   Resultado: ANORMAL
Entrada:   -1.000   -0.640   Resultado: NORMAL
Entrada:   +1.000   -0.640   Resultado: ANORMAL
Entrada:   -0.420   -1.078   Resultado: NORMAL
Entrada:   -0.420   +1.078   Resultado: ANORMAL
Entrada:   -1.045   -1.089   Resultado: NORMAL
Entrada:   +1.045   +1.089   Resultado: ANORMAL
Entrada:   -1.068   -1.000   Resultado: NORMAL
Entrada:   +1.068   -1.000   Resultado: ANORMAL
Entrada:   -1.068   -1.040   Resultado: NORMAL
Entrada:   +1.068   +1.040   Resultado: ANORMAL
Entrada:   -1.045   -1.089   Resultado: NORMAL
Entrada:   -1.045   +1.089   Resultado: ANORMAL
```

A tabela 9.6 resume os valores dos fluxos nas linhas conectados às barras 4 e 6 e obtidos através do Módulo Estimador de Estados.

O gráfico da figura 9.18 apresenta uma comparação dos valores obtidos através do Módulo de Estimação de Estados para os dois primeiros exemplos da Tabela 9.6. Podemos constatar a discrepância entre os valores obtidos nas 2 séries apresentadas neste gráfico para as linhas 4-1 (coluna 1), 4-2 (coluna 2) e 4-5 (coluna 3). Considerando a capacidade nominal para as linhas 4-1, 4-2 e 4-5 respectivamente 50 MW, 40 MW, e 10 MW, a linha 4-5 estaria cerca de 40% além da sua capacidade nominal (141/10=1.40). Caso o operador considerasse os resultados apresentados pelo estimador de estados, ele poderia ser levado a pensar que havia uma sobrecarga na capacidade desta linha. Diferentemente, o Detector de Anomalias classificou este exemplo como Anormal, apontando para uma possível corrupção dos valores lidos do sistema SCADA. Os exemplos subseqüentes apresentaram da mesma forma discrepâncias de valores (ver figuras 9.19 até 9.23). Em alguns casos houve até inversão do fluxo de potência da linha (ver figuras 9.21, 9.22 e 9.23).

Tabela 9.6 - Resumo dos resultados do Caso 2 obtidos pelo Detector de Anomalias e o Módulo Estimador de Estados

IMW4	IMW6	4 to 1	4 to 2	4 to 5	6 to 1	6 to 3	6 to 5	Tipo de Erro Introduzido	Status do Detector
-0.310	**-0.700**	-22.19	-17.74	+8.93	-26.59	-42.73	-0.67	SEM ERRO	NORMAL
+0.310	**-0.700**	-12.99	-2.21	+14.00	-29.73	-42.61	-0.93	TROCA DE SINAL	ANORMAL
-0.700	**-0.430**	-34.18	-38.43	+2.61	-14.84	-33.29	+5.13	SEM ERRO	NORMAL
-0.700	**+0.430**	-33.63	-42.74	+1.78	-0.67	-14.19	+14.52	TROCA DE SINAL	ANORMAL
-0.480	**-0.423**	-22.47	-30.55	+5.01	-15.03	-33.03	+5.72	SEM ERRO	NORMAL
+0.480	**+0.423**	-7.54	-10.93	+12.02	-6.04	-14.01	+14.60	TROCA DE SINAL	ANORMAL
-0.9799	**-0.610**	-54.20	-44.56	+0.77	-21.58	-39.65	+0.23	SEM ERRO	NORMAL
-0.9799	**+0.610**	-53.48	-50.68	-0.41	-1.53	-12.56	+13.49	TROCA DE SINAL	ANORMAL
-0.999	**-0.6399**	-56.08	-44.59	+0.77	-22.76	-40.71	-0.52	SEM ERRO	NORMAL
+0.999	**-0.6399**	-27.12	+5.59	+17.17	-33.16	-40.32	-1.35	TROCA DE SINAL	ANORMAL
-0.420	**-1.078**	-39.75	-12.78	+10.52	-41.75	-56.05	-10.0	SEM ERRO	NORMAL
-0.420	**+1.078**	-38.38	-23.68	+8.47	-6.73	-8.16	+13.32	TROCA DE SINAL	ANORMAL
-1.045	**-1.089**	-72.10	-35.94	+3.54	-40.99	-56.56	-11.35	SEM ERRO	NORMAL
+1.045	**+1.089**	-40.92	+5.81	+18.87	-16.74	-7.74	+11.25	TROCA DE SINAL	ANORMAL
-1.0678	**-1.000**	-70.52	-38.87	+2.61	-37.32	-53.42	-9.26	SEM ERRO	NORMAL
+1.0678	**-1.000**	-39.94	15.14	20.29	-48.26	-53.06	-10.20	TROCA DE SINAL	ANORMAL
-1.0678	**-1.0395**	-71.73	-37.95	+2.91	-38.93	-54.82	-10.20	SEM ERRO	NORMAL
+1.0678	**+1.0395**	-39.94	+5.42	+18.69	-16.48	-8.18	-11.33	TROCA DE SINAL	ANORMAL
-1.045	**-1.0899**	-72.10	-35.94	+3.54	-40.99	-56.56	-11.35	SEM ERRO	NORMAL
-1.045	**+1.0899**	-70.95	-46.95	+1.46	-5.61	-9.19	+12.14	TROCA DE SINAL	ANORMAL

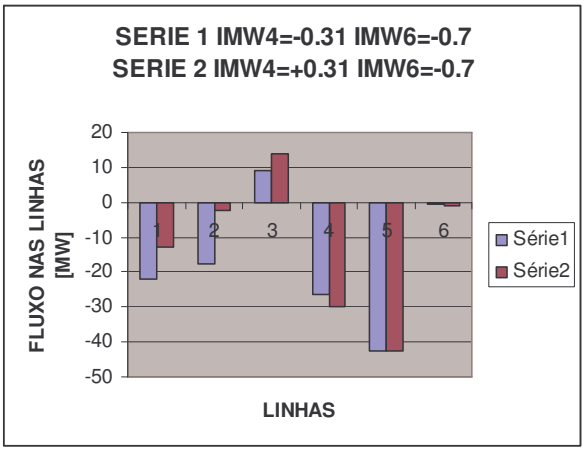


Figura 9.18 - Comparando resultados sem dados corrompidos (serie 1) e com dados corrompidos (serie2)

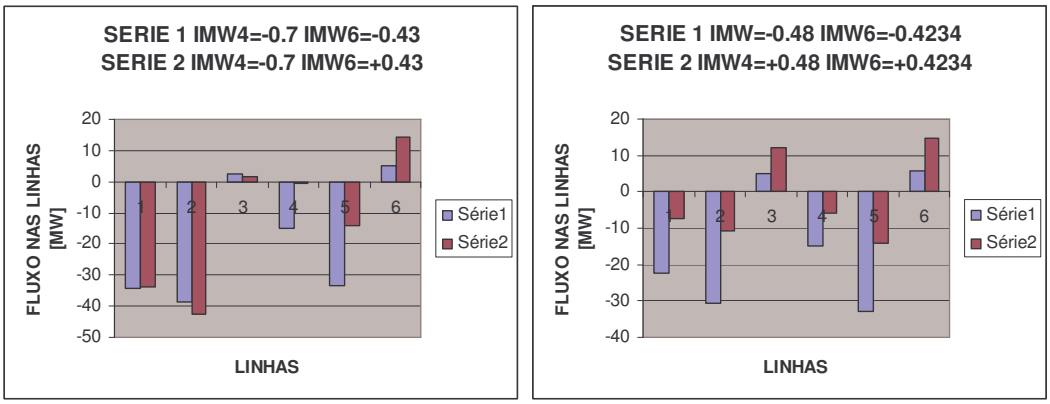


Fig. 9.19: Comparando resultados sem dados corrompidos (serie 1) e com dados corrompidos (serie2)

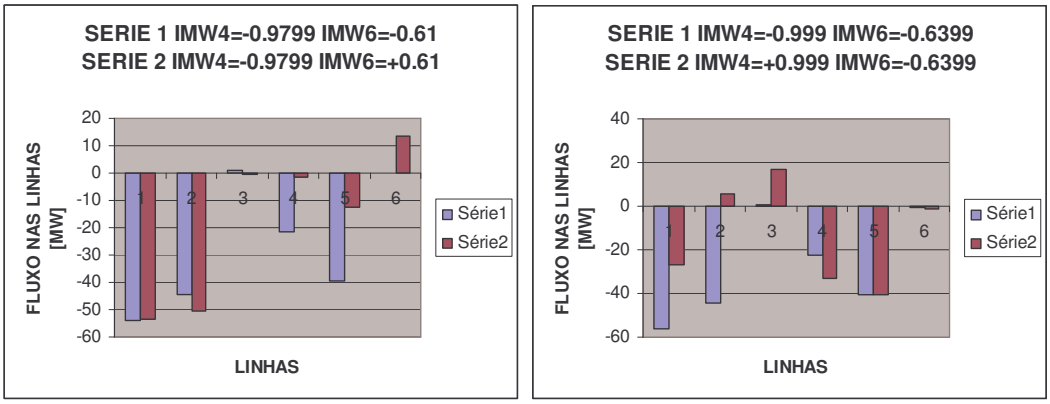


Figura 9.20 - Comparando resultados sem dados corrompidos (serie 1) e com dados corrompidos (serie2)

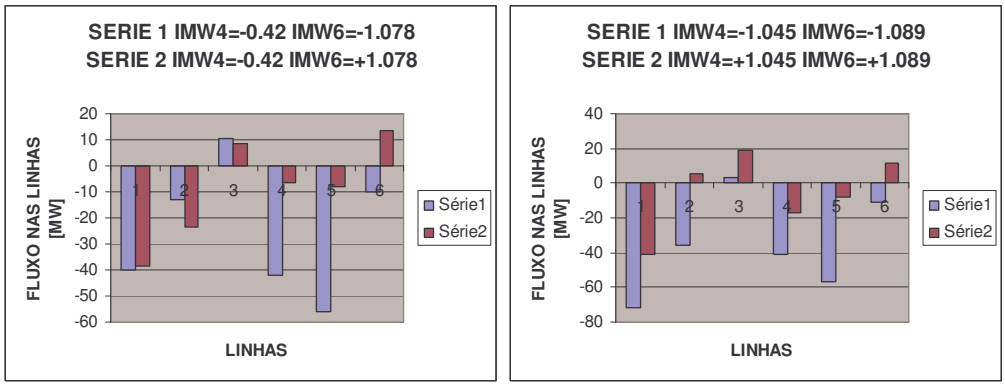


Figura 9.21- Comparando resultados sem dados corrompidos (serie 1) e com dados corrompidos (serie2)

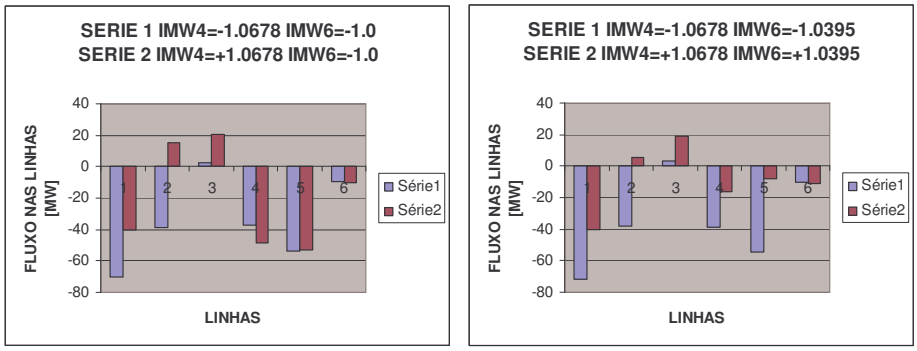


Figura 9.22- Comparando resultados sem dados corrompidos(serie 1) e com dados corrompidos(serie2)

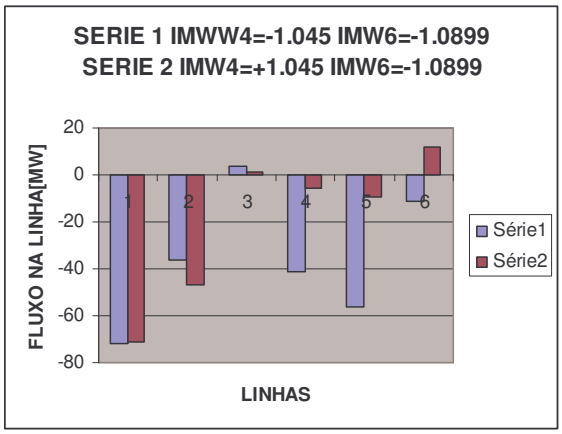


Figura 9.23- Comparando resultados sem dados corrompidos (serie 1) e com dados corrompidos (serie2)

Da mesma forma que no caso teste anterior, se o operador considerar somente os resultados apresentados pelo estimador de estados, a estabilidade do sistema poderia vir a ser ameaçada. Com a ajuda do Detector de Anomalias, que classificou estes exemplos como Anormal, o operador poderia ser alertado para uma possível corrupção dos valores lidos do sistema SCADA.

9.5.1 Estudo de Caso 3: Corrompendo o Valor de Tensão

Neste novo caso teste, será abordado a corrupção do valor de tensão nas barras 4 e 6 e sua influência no modelo operacional proposto. A idéia foi alterar os valores de tensão nestas barras e verificar se o detector de anomalias classifica esta nova situação

como anormal e como o estimador de estado vê esta nova situação. Para tanto um novo arquivo de configuração de medidores foi definido. Neste arquivo 2 novos medidores de tensão foram incluídos nas barras 4 e 6.

Primeiramente foram simulados no ambiente de testes diversos exemplos onde se procurou variar os valores de potência ativa nas barras 4 e 6. A faixa de variação da potência em ambas as barras foi de 0.3 pu até 1.8 pu, em intervalos de 0.1 pu. A seguir foram adulterados os valores de tensão no arquivo produzido pelo Simulador SCADA. O tipo de erro introduzido foi definir um novo valor de tensão nas barras 4 e 6 com um valor 10% menor que o valor original. A listagem abaixo apresenta um trecho do arquivo SCADA para um exemplo e o erro introduzido. Veja no Anexo E.1 a listagem original completa.

```
LINE    1    2  1.00000E-01  2.00000E-01  2.00000E-02
LINE    1    4  5.00000E-02  2.00000E-01  2.00000E-02
LINE    1    5  8.00000E-02  3.00000E-01  3.00000E-02
LINE    2    3  5.00000E-02  2.50000E-01  3.00000E-02
LINE    2    4  5.00000E-02  1.00000E-01  1.00000E-02
LINE    2    5  1.00000E-01  3.00000E-01  2.00000E-02
LINE    2    6  7.00000E-02  2.00000E-01  2.50000E-02
LINE    3    5  1.20000E-01  2.60000E-01  2.50000E-02
LINE    3    6  2.00000E-02  1.00000E-01  1.00000E-02
LINE    4    5  2.00000E-01  4.00000E-01  4.00000E-02
LINE    5    6  1.00000E-01  3.00000E-01  3.00000E-02
V    1     1.0500000000E+00  1.000E-04
V    4     9.9757488501E-01  1.000E-04
V    6     9.8744382133E-01  1.000E-04
A    1     0.0000000000E+00  1.000E-04
A    4    -3.1603824341E-02  1.000E-04
A    6    -7.2849142749E-02  1.000E-04
I    1     6.5929218705E-01  1.000E-02     2.6187809122E-01  1.000E-02
I    2     5.0000093699E-01  1.000E-02     8.8506883860E-01  1.000E-02
```

Valores de Tensão para as barras 4 e 6 adulterados neste ponto para 0.89775 (V4) e 0.8886 (10 % menor que o valor original) respectivamente.

Foi produzida uma base de conhecimento com 170 exemplos, cada exemplo com 59 valores. Estes exemplos foram classificados como um Caso Normal ou como um Caso Anormal, dependendo dos valores de tensão. Esta base de conhecimento foi lida pelo módulo extrator de regras e produziu as seguintes regras:

- **IF (V4>=0.9217) & (V4<0.9977) & (V6>=0.9071) & (V6<1.0007) Resultado = Normal;**
- **IF (V4>=0.8459) & (V4<0.9217) Resultado = Anormal;**
- **IF (V6)>=0.8135) & (V6<0.9071) Resultado = Anormal;**

- **IF(V4>=0.77) & (V4<0.8459) Resultado = Anormal;**
- **IF (V6>=0.72) & (V6<0.8135) Resultado = Anormal;**

Este conjunto de regras foi implementado em Matlab (veja Anexo E.2 para listagem) e testado com um arquivo contendo 10 exemplos testes (veja Anexo E.3). A saída para este caso teste é apresentada abaixo (Anexo E.4):

```
» regrasdb1
Entre com nome do arquivo de dados: 'caso_tensao_teste.txt'
Entre com número de entradas: 10
Entre com número de colunas: 59
                    V4         V6
Entrada:     1   +0.994   +0.985   Resultado: NORMAL
Entrada:     2   +0.900   +0.850   Resultado: ANORMAL
Entrada:     3   +0.982   +0.960   Resultado: NORMAL
Entrada:     4   +0.882   +0.910   Resultado: ANORMAL
Entrada:     5   +0.929   +0.916   Resultado: NORMAL
Entrada:     6   +0.829   +0.906   Resultado: ANORMAL
Entrada:     7   +0.922   +0.926   Resultado: NORMAL
Entrada:     8   +0.902   +0.826   Resultado: ANORMAL
Entrada:     9   +0.921   +0.946   Resultado: ANORMAL
Entrada:    10   +0.721   +0.846   Resultado: ANORMAL
```

As listagens do Anexo E.5 e E.6 apresentam os resultados do módulo de estimação de estados para o caso onde a potência ativa, para as barras 4 e 6, foi fixada em 0.55 pu e 1.05 pu, respectivamente. E.5 representa o caso sem adulteração de dados e E.6 representa o caso com adulteração dos valores de tensão na barra 4 e na barra 6. Os valores apresentados para potência ativa, potência reativa e potência aparente estão comparados no gráfico da figura 9.24. Nos casos apresentados, os valores de tensão foram adulterados de V4=0.982 pu para V4=0.882 pu e de V6=0.960 pu para V6=0.910 pu. O módulo de detecção de anomalias classificou corretamente como Normal o exemplo com os valores originais e Anormal o exemplo com os valores corrompidos. Veja entrada 3 e 4 na listagem do Anexo E.4.

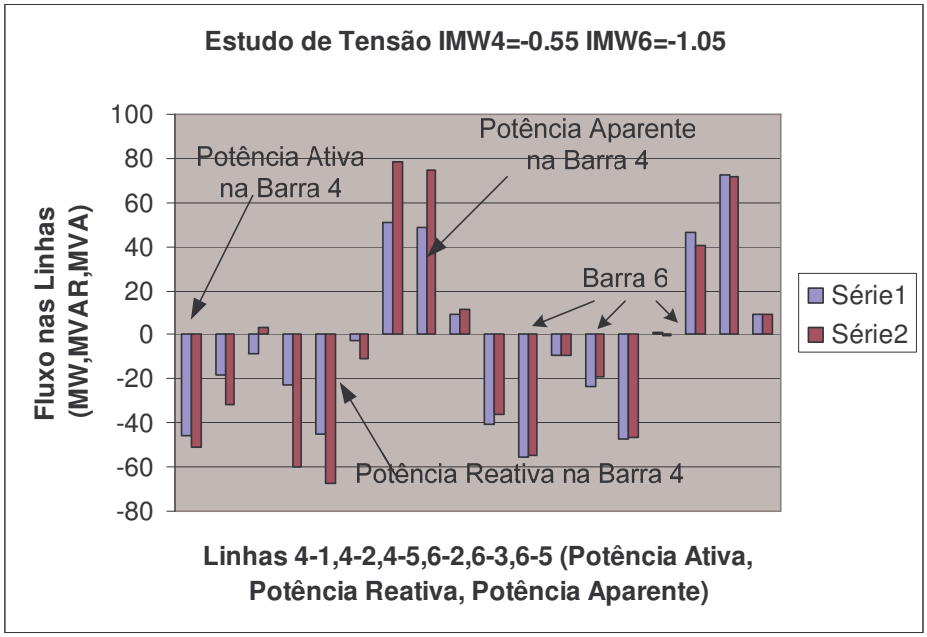


Figura 9.24 – Comparando resultados da saída do estimador de estados para testes sem corrupção (Série 1) e com corrupção (Série 2) de tensão nas barras 4 e 6.

Das listagens dos Anexos E.5 e E.6, observa-se os seguintes valores para a Potência Aparente (em MVA):

Caso	**4 para 1 (MVA)**	**4 para 2 (MVA)**	**4 para 5 (MVA)**	**6 para 2 (MVA)**	**6 para 3 (MVA)**	**6 para 5 (MVA)**
Sem corrupção	50.76	48.67	9.18	46.72	72.56	9.61
Com corrupção	78.49	74.57	11.56	40.68	71.54	9.17

A análise dos resultados revelou que em termos da variação dos resultados, a potência reativa e a potência aparente para a barra 4 tiveram maiores discrepâncias entre os valores originais e os valores corrompidos pela mudança do valor da tensão. A potência ativa nas duas barras não apresentou variações que pudessem chamar a atenção. Isto se deve ao fato de que houve, neste caso, a corrupção dos valores da

magnitude da tensão nas barras 4 e 6, diferentemente dos casos anteriores, onde ocorreu corrupção dos valores do fluxo de potência ativa nas linhas conectadas às barras 4 e 6. Vale ressaltar que a potência ativa sofre forte influência do ângulo da tensão enquanto que a potência reativa sofre ação direta da magnitude da tensão. Como a potência aparente é calculada através da fórmula:

$$S= P + jQ$$

Pode-se dizer que os valores adulterados da magnitude da tensão acabaram por afetar a potência aparente também.

Como ocorreu com os outros casos testes analisados anteriormente, o módulo de estimação de estados apresentou resultados que poderiam vir a fazer com que o operador tomasse medidas para corrigir a condição de operação do sistema, tendo em vista os resultados apresentados por este módulo nos Anexos E.5 e E.6. Como o que realmente aconteceu foi a adulteração das informações coletadas pelo Sistema SCADA, as medidas tomadas pelo operador poderiam vir a por em perigo a estabilidade do sistema elétrico de potência. O módulo de detecção de anomalias implementado pelas regras extraídas da base de conhecimento classificou corretamente estas entradas como anormais, evitando a interpretação errônea. Mais resultados deste estudo de caso são apresentados na figura 9.25 e 9.26. Estes casos representam o mesmo fato relatado na figura 9.24. Novamente o módulo de detecção de anomalias classificou estes casos corretamente, conforme a listagem apresentada no Anexo E.4.

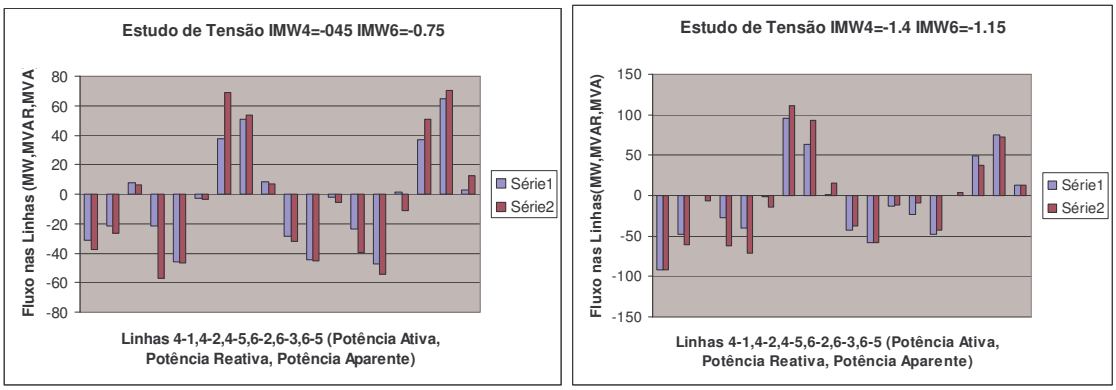


Figura 9.25 – Comparando resultados da saída do estimador de estados para testes sem corrupção (Série 1) e com corrupção (Série 2) de tensão nas barras 4 e 6.

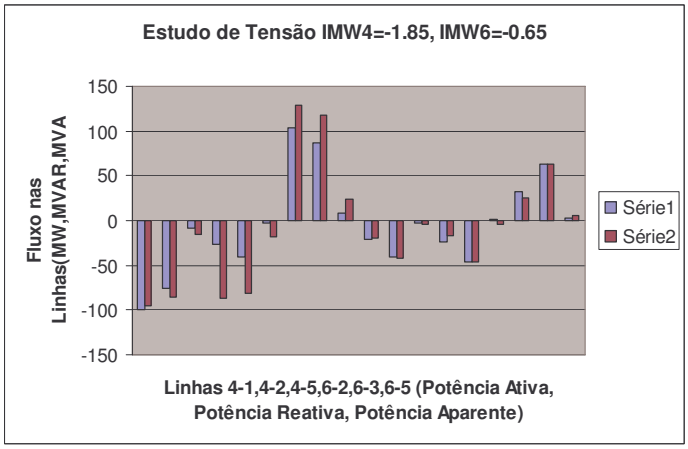


Figura 9.26 – Comparando resultados da saída do estimador de estados para testes sem corrupção (Série 1) e com corrupção (Série 2) de tensão nas barras 4 e 6.

CAPITULO 10

CONCLUSÕES E FUTUROS TRABALHOS

O aumento da interconectividade entre os Centros de Operação do Sistema Elétrico (COS), as redes corporativas dos Agentes e a Internet, tem tornado a camada cibernética da Infra-estrutura Crítica do Sistema Elétrico de Potência cada vez mais vulnerável a atacantes externos e externos ao Sistema. Esta tendência tem sido acelarada pelo uso cada vez maior de software comercial e de redes padrão TCP/IP/Ethernet. Embora o uso dos tradicionais sistemas de detecção de intrusão, programas anti-virus e "*firewalls*" sejam indicados para proteger esta infra-estrutura contra os ataques cibernéticos, os produtos baseados em assinaturas possuem capacidade limitada na detecção e na defesa contra as novas e inovadoras formas de ataques e descritas no Capitulo 5. Para melhorar e complementar o desempenho desta metodologia foi proposto o modelo de detecção de anomalias usando técnicas inteligentes que aprende o comportamento normal do sistema, constrói uma base de conhecimentos que define o perfil operacional do sistema e, finalmente, detecta as operações anômalas que se desviam deste perfil. Este modelo é, então, utilizado para melhorar o processo de estimação de estado, informando aos operadores sobre as discrepâncias encontradas entre a sua visão da rede e o estado real de operação. Detecção por anomalia detecta qualquer mudança anormal, seja ela produzida por "*bugs*" no software operacional, atacantes ou qualquer outra condição estranha à rede elétrica. Isso seria muito útil para chamar a atenção dos operadores antes que possam ameaçar a estabilidade do sistema.

O presente trabalho abordou em seu Capítulo 8 os aspectos de detecção de intrusão por anomalias em sistemas elétricos de potência. Foram descritas algumas técnicas utilizadas para implementar o algoritmo de análise de detecção e apresentada a proposta do algoritmo de detecção de anomalias usando a Teoria de Conjuntos Aproximados. No Capitulo 9 apresentou-se a implementação da arquitetura do detector de anomalias proposto. De tal forma a validar a proposição foi criado um ambiente de testes composto dos módulos de fluxo de carga, simulador SCADA, módulo estimador de estados, módulo extrator de regras usando a teoria dos conjuntos aproximados e o módulo do detector de anomalias. Os resultados obtidos para os casos testes implementados foram satisfatórios comprovando a eficiência do algoritmo proposto e vindo a reforçar a afirmação anterior sobre a melhoria do processo de estimação de estados para os operadores.

Através do estudo de casos desenvolvido no Capitulo 9, constatou-se a simplicidade das regras obtidas com o módulo extrator de regras, a partir da base de conhecimentos montada em cada estudo de caso. Para estes estudos foram utilizados os dados do sistema elétrico de potência de 6 barras proposto em [140]. O Cenário de Ataque incluiu a corrupção do Sistema SCADA com a troca de sinal nas medidas de potência ativa na Barra 4 e na Barra 6 do sistema elétrico proposto. Também foram feitos estudos da influência da corrupção dos valores de tensão coletados pelo sistema SCADA no estimador de estados. Em todos os casos o detector de anomalias, implementado a partir das regras extraídas da base de conhecimento, classificou corretamente os eventos anormais e normais, fornecendo uma eficiência de 100% para todos os casos.

10.1 PRINCIPAIS CONTRIBUIÇÕES

Dentre as principais contribuições deste trabalho destaca-se:

1) Importância da Proteção Cibernética de Infra-estruturas Críticas, especificamente, aquela relacionada com Sistema Elétrico de Potência.
2) Importância da Proteção Cibernética de Sistemas SCADA em sistemas elétricos de potência através do uso de Detectores de Anomalias.
3) Eficiência do modelo de análise para o detector de anomalias usando o algoritmo dos conjuntos aproximados. O modelo demonstrou sua eficácia na especificação de regras simples a partir da base de conhecimento gerada. As regras implementadas detectaram com sucesso as corrupções produzidas nos dados coletados pelo sistema SCADA (simulado aqui pelo módulo Simulador de SCADA).
4) Devido a simplicidade das regras obtidas, o módulo detector de anomalias requer baixo recurso computacional para sua implementação. Isto é de suma importância tendo em vista a limitação dos recursos computacionais existentes nos módulos SCADA,UTRs, IEDs e PLCs.

10.2 PERSPECTIVAS FUTURAS

A atual implementação do detector de anomalias faz somente a classificação dos exemplos em Evento Normal e Evento Normal. Numa próxima etapa deste trabalho, pode-se implementar outro modelo em que o tipo de erro introduzido seja identificado. Desta forma o tipo de ataque poderia vir a ser identificado. Em estudos anteriores, outros autores propuseram a correlação da saída do detector de anomalias com o detector de intrusão baseado em assinaturas. Esta técnica permite a identificação do tipo

de ataque, visto que ambas condições, tráfego de rede e fluxo de dados do sistema, serão analisados em conjunto. Entretanto uma vantagem do modelo usado com conjuntos aproximados é que tal método permite a classificação dos eventos anormais em vários tipos eventos, tais como, com corrupção por sinal, valor fixado, etc..

REFERÊNCIAS BIBLIOGRÁFICAS

[1] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 – USA PATRIOT ACT of 26 October 2001", http://www.epic.org/privacy/terrorism/hr3162.pdf.

[2] "The National Strategy to Secure Cyberspace", Washington D.C., February, 2003, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

[3] "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", Washington D.C., Feb 2003, http://www.dhs.gov/interweb/assetlibrary/ Physical_Strategy.pdf.

[4] Luiijf, E.A.M., Klaver,M.H.A., "International Interdependency of C(I)IP in Europe (Internationale Verflechtung von C(I)IP in Europa)", Clingendael Center for Strategic Studies (CCSS), TNO Defence, Security and Safety, CIP Europe 2005/Informatik 2005, 19/05/2005, Bonn, Germany, http://www.tno.nl/defensie_en_veiligheid/ producten_en_diensten/beleidsstudies/veiligheid/information_operations/Paper_luiijf_v 5.pdf

[5] Bruce, R. et all, "TNO Report - International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues", Center for Digital Strategies, Tuck School of Business at Dartmouth, 2005, http://cds-1.dartmouth.edu/docs/discussion_paper_final.pdf.

[6] Gamez,D., Nadjm-Tehrani, S., Bigham, J., Balducelli, C., Burbeck, K., Chyssler, T., "Chapter 19 Safeguarding Critical Infrastructures", Edited by Professor Hassan B. Diab & Professor Albert Y. Zomaya , "Dependable Computing Systems: Paradigms, Performance Issues, and Applications" , Wiley STM, 2000.

[7] “Homeland Security Act of 2002”, Washington D.C., January, 2002, http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf.

[8] “Trusted Computer System Evalation Criteria-(Orange Book)”, http://www.boran.com/security/tcsec.html.

[9] “Information Technology Security Evaluation Criteria – ITSEC” http://www.bsi.bund.de/zertifiz/itkrit/itsec-en.pdf.

[10] “Iformation Technology Security Evaluation Manual – ITSEM”, http://www.bsi.bund.de/zertifiz/itkrit/itsem-en.pdf.

[11] “Common Criteria for Information Technology Security Evaluation CCITSE”, http://www.bsi.bund.de/cc/index.htm.

[12] IT-Grundschutz Manual 2004, http://www.bsi.bund.de/english/gshb/index.htm.

[13] Byres, E. and Lowe, J., “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems”, VDE 2004 Congress, VDE, Berlin, October, 2004.

[14] Falco, J., Stouffer, K., Wavering, A., Proctor, F., “IT Security for Industrial Control Systems”, NISTIR 6859, February 2002, http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf.

[15] Dunn, M. Wigert, I., “International CIIP Handbook 2006 Vol. I and II“, Eidgenössische Technische Hochschule Zürich (ETHZ), Zürich, 2006, http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=16156.

[16] “Critical Foundations: Protecting America’s Infrastructures”, Report from the President’s Commission on Critical Infrastructure Protection”, Washington D.C., 1997.

[17] “National Plan for Information Infrastructure Protection”, Federal Ministry of the Interior, Germany, October 2005, http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National_

_Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.

[18] "CI2RCO - Critical Information Infrastructure Research Co-ordination", http://www.ci2rco.org/.

[19] Bezerra, E.K., Nakamura, E. T., Lima, M.B., "Necessidade e deasafios para definição de um metodologia para proteção de Infra-estrutura Crítica de Telecomunicações", CPqD – Centro de Pesquisa e Desenvolvimento-Telecom & IT Solutions, Campinas, Brasil.

[20] Bezerra, E.K., Nakamura, E. T., Lima, M.B., "Proteção da Infraestutura Crítica de Telecomunicações: Análise, Metodologia e Aplicações", 6° Simpósio Segurança em Informática, 09/11 a 12/11/2004, Instituto Tecnológico de Aeronáutica – ITA, São José dos Campos, SP , http://www.linorg.cirp.usp.br/SSI/SSI2004/Poster/P02_ssi04.pdf.

[21] Goetz, E., "Cyber Security of the Electric Power Industry", Institute for Security Technology Studies at Dartmouth College", Dartmouth, USA, December, 2002.

[22] Byres, E. and Lowe, J., "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE 2004 Congress, VDE, Berlin, October, 2004.

[23] "Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electric Power Systems", Texas A & M Annual Conference for Protective Relays Engineers, April, 2002.

[24] Oman, P., Schweitzer, E., and Roberts, J., "Protecting the Grid from Cyber Attack, Part II: Safeguarding IEDS, Substations and SCADA Systems", Utility Automation, 7(1), 2002, pp. 25-32.

[25] "National Energy Policy", Report of the National Energy Policy Development Group, Report of the National Energy Policy Development Group, Washington-DC,

http://www.whitehouse.gov/energy/Chapter7.pdf, USA, May, 2001, ISBN: 0-16-050814-2.

[26] Shainker, R., Douglas, J., Kropp, T., “Electric Utility Responses to Grid Security Issues”, IEEE Power & Energy Magazine, March/April 2006, USA.

[27]”The Energy Policy Act 2005”, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00006:

[28] ”The Security Guidelines for the Electricity Sector”, http://www.esisac.com/library-guidelines.htm.

[29] “Cyber Security Standards CIP-002-1 through CIP-002-9”, http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html.

[30]Amin, M., “North America´s Electricity Infrastructure: Are we ready for more perfect storms?” , IEEE Security & Privacy, September/October 2003, USA.

[31] ”Livro de Referência sobre a infra-estrutura crítica do Brasil”, SECGOV-2006, Janeiro 2007, Brasil, http://www.secgov.com.br/Livro_Branco.aspx.

[32] “RFC 791 – Internet Protocol”, September, 1981, http://www.rfc-editor.org/.

[33] Hall, Eric A.,”Internet Core Protocols: The definitive guide”, ISBN 1-56592-572-6, O´Reilly & Associates, Inc, 2000.

[34]Dzung, D., Naedele, M., Von Hoff, T.P., Crevatin, M., “Security for Industrial Communications Systems”, Proceedings of the IEEE, Vol.93,No. 6, June 2005.

[35] Tipsuwan, Y., Chow,Mo-Yuen, “Control Methodologies in Newtworked Control Systems”, Control Engineering Practice 11 (2003) 1099-1111, Elsevier Ltd. http://www4.ncsu.edu/%7Echow/Publication_folder/Journal_paper_folder/2003_NBC_Tutorial_Yod.pdf.

[36]"Overview and Introduction to the Manufacturing Message Specification (MMS)", http://www.sisconet.com/downloads/mmsovrlg.pdf.

[37] "OPC Overview", http://www.opcfoundation.org/Archive/72e9fbfa-6a89-4ef2-9b6d-3f746fd7eb05/General/OPC%20Overview%201.00.pdf.

[38] Chucre, Marcelo M., "Programação e Compatibilização de uma Rede Padrão Profibus", Dissertação de Mestrado, Escola Federal de Engenharia de Itajubá, Setembro/1997.

[39] Hansman, S., "A Taxonomy of Network and Computer Attack Methodologies", Supervisor: Ray Hunt, Department of Computer Science and Software Engineering, University of Cantebury, Christchurch, New Zealand, November, 2003, http://coscweb2.cosc.canterbury.ac.nz/research/reports/HonsReps/2003/hons_0306.pdf.

[40] Arbaugh, W.A., Fithen, W.L., McHugh, J.,"Windows of Vulnerability: a Case Study Analysis", IEEE Computer, Volume 33, Issue 12, pp.52 – 59, Dec. 2000.

[41]Anderson, JP, "Computer Security Threat Monitoring and Surveillance", Technical Report, 1980, http://seclab.cs.ucdavis.edu/projects/history/CD/ande80.pdf.

[42] Mahan, Robert, E., "Security Vulnerabilities & Loopholes: Chapter 11 Security Vulnerabilities",http://www.tricity.wsu.edu/htmls/cs427/public_html/Ch%2011%20Security%20Loopholes.pdf, , January, 2000.

[43] Jelatis, G.D., Weiss, J., "Information Security Primer", EPRI Report, 2000.

[44] Byres, E., Carter, J., Elramly, A., Hoffman, D.,"Worlds in Collision - Ethernet and the Factory Floor", ISA 2002 Emerging Technologies Conference, Instrumentation, Systems and Automation Society, Chicago, Ocotober, 2002, http://www.bcit.ca/files/appliedresearch/pdf/security/worldsincollision.pdf.

[45] Schneier, B., “Applied Criptgraphy”, 2nd Ed., New York, Wiley & Sons, 1996.

[46] Bigham, J., Gamez, D., Ning Lu, “Safeguarding SCADA Systems with Anomaly Detection”, V.Gorodetsky et al. (Eds.):MMM-ACNS 2003, LNCS 2776, pp. 171-182, Springer-Verlag Berlin Heidelberg, 2003.

[47] Oman, P., Schweitzer,III, O., Roberts, J., “Safeguarding IEDs, Substations,and SCADA Systems Against Electronic Intrusions“ , Proceedings of the 2001 Western Power Delivering Automation Conference, Paper No. 1, April 9-12, Spokane, WA, 2001, http://www.selinc.com/techpprs/6118.pdf.

[48] Naedele, M., Dzung, D., “Industrial Information System Security, Part 1”, ABB Review 2/2005.

[49] “Electric Power Information Assurance Risk Assessment”, National Security Telecommunications Advisory Committee, Information Assurance Task Force, March, 1997, http://www.securitymanagement.com/library/iatf.html.

[50] CERT, “Cyber Threats, Trends and Strategies”, Carnegie Mellon University, http://www.cert.org/archive/ppt/cyberterror.ppt.

[51] Eisenhauer, J., Donelly, P., Ellis, M., O’Brien, M., “Roadmap to Secure Control Systems in the Energy Sector“, January 2006, http://www.controlsystemsroadmap.net.

[52] Bakken, D., Hauser, C., Bose, A., ”GridStat Middleware for more Extensible and Resilient Status Dissemination for the Electric Power Grid”, School of Electrical Engineering and Computer Science, Washington State University, Pullman, Washington, USA, November 2003, http://www.gridstat.net/overview.php.

[53] Barnes, K., Johnson, B., “Introduction to SCADA Protection and Vulnerabilities”, Idaho National Engineering and Environmental Laboratory, January2004, INEEL/EXT-04-01710, http://www.inl.gov/technicalpublications/Documents/3310860.pdf.

[54] Byres, E.J., “Designing Secure Networks for Industrial Controls”, IEEE Industrial Applications Magazine, Vol.6, No.5, Sep-Oct 2000, pp. 33-39, http://www.bcit.ca/files/appliedresearch/pdf/ieee99_processlan_protection.pdf.

[55] Hause, C.H., Bakken, D.E., Bose, A.,”Failure do Communicate”, IEEE Power & Energy Magazine, March-April 2005, pps. 47-55.

[56] Gjermundrod, K.H., Dionysiou, I., Bakken,D., Hauser, C., Bose, A., “Flexible and Robust Status Dissemination Middleware for the Electric Power Grid”, Technical Report EECS-GS-003, School of Electrical Engineering and Computer Science, Washington State University, September 25, 2003, Pullman, Washington, USA, http://www.gridstat.net/publications/GridStat-EECS-GS-003.pdf.

[57] Bose, A., “Power System Stability: New Opportunities for Control”, Chapter in Stability and Control of Dynamical Systems and Applications, Derong Liu and Panos J. Antsaklis, Editors, Birkhauser (Boston), 2003, http://www.gridstat.net/ publications/Bose-GridComms-Overview-Chapter.pdf.

[58] Tomsovic,K., Bakken,D., Venkatasubramanian, V., Bose, A., “Designing the Next-Generation of Real-Time Control, Communication and Computations for Large Power Systems”, Proceedings of the IEEE, Vol. 93, No.5, May 2005, pps. 965-979.

[59] Procedimentos de Rede - Operador Nacional do Sistema Elétrico, http://www.ons.org.br/procedimentos.

[60] Berg, M., Stamp, J., “A Reference Model for Control and Automation Systems in Electric Power”, Sandia National Laboratories Report SAND2005-1000C, 2005, http://www.sandia.gov/scada/documents/sand_2005_1000C.pdf.

[61]Barnes,K., Johnson, B., Nickelson, R., “Review of Supervisory Control and Data Acquisition (SCADA) Systems”, Idaho National Engineering and Environmental

Laboratory (INEEL), January 2004, INEEL/EXT-04-01517, http://www.inl.gov/technicalpublications/Documents/3310858.pdf.

[62] Naedele, M., "Addressing IT Security for Critical Control Systems", 40th Hawaii Int. Conf. on System Sciences (HICSS-40) Hawaii, January 2007.

[63] "IntelliGrid Project Home Page", http://www.intelligrid.info/.

[64] "Good Practice Guide on Firewall Deployement for SCADA and Process Control Networks", National Infrastructure Security Coordination Centre – NISCC, British Columbia Institute of Technology – BICT, Group for Advanced Information Technology (GAIT), February, 2005.

[65] Naedele, M., "Sicherheit in Automatisierungssystem fur Energiesorger", ew, Vol.104(11), 5/2005, pp. 56-61.

[66] Marin,G.A., "Network Security Basics", IEEE Security & Privacy, November/December, 2005.

[67] Risley, A., Roberts, J., LaDow, P., "Electronic Security of Real-Time Protection and SCADA communications", Schweitzer Engineering Laboratories, Inc., Pullman, Washington, USA, 2003.

[68] Holstein, D. K., Diaz, J., "Cyber Security Management for Utility Operations", 39th Annual Hawaii International Conference on System Sciences – HICSS'06.

[69] Naedele, M., "Standardizing Industrial IT Security – A First Look at the IEC Approach", 10th IEEE Conference on Emerging Tecnologies and Factory Automation, Vol. 2, 19-22 September, 2005, pp. 857-863.

[70] Katzke, S., Stouffer, K., Abrams, M., Norton, D., Weiss, J., "Applying NIST SP 800-53 to Industrial Control Systems", ISO EXPO 2006.

[71] Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., " NIST SP 800-53 Recommended Security Controls for Federal Information Systems", http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

[72] Stoufer, K., Falco, J., Kent, K., "NIST Draft SP 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security", http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf.

[73] Watts, D., "Security & Vulnerability in Electric Power Systems", NAPS 2003, 36th North American Power Symposium, Univeristy of Missouri-Rolla , October 20-21, 2003, pp. 559-566, Rolla, Missouri, USA.

[74] Filho, X.V., Pilotto, L.A.S., Martins, N., Cravalho, A.R.C., Bianco, A., "Brazilian Defense Plan against Extreme Contigencies", IEEE Power Engineering Society Summer Meeting, 2001, Vol. 2, 15-19 July 2001, pp. 834-839.

[75]Oman, P., Schweitzer, E. O., Frinke, D.,"Concerns About Intrusions into Remotely Accessible Substations Controllers and SCADA Systems", 27th Annual Western Protective Relay Conference, Paper #4, Ocotober 23-26, 2000, Spokane, WA, USA.

[76] Hale, J., Bose, A., "Information Survivability in Electric Utility Industry", ISW'98, http://www.cert.org/research/isw/isw98/all_the_papers/no19.html.

[77] "21 Steps to improve Cyber Security of Scada Networks", http://www.esisac.com/publicdocs/21StepsBooklet.pdf.

[78] Amanullah, M.T.O., Kalam, A., Zayegh, A., "Network Security Vulnerabilities in SCADA and EMS", 2005 IEEE/PES Transmission and Distribution Conference & Exhibition : Asia and Pacific, Dalian, China.

[79] Ericssom,G. N., Torkilsend. A.,"Management of Information Security for an Electric Power Utility – On Security Domains and Use of ISO/IEC 17799 Standard", IEEE Trans. On Power Delivery, Vol. 20, No. 2, April 2005.

[80] Geer, D., “Security of Critical Control Systems Sparks Concern”, IEEE Computer, Vol. 39, Issue 1, January 2006, pp. 20-23.

[81] Naedele, M., Dzung D., Stanimirov, M., “Network Security for Automation Systems”, SAFECOMP 2001, LNCS 2187, pp. 25-34, Springer-Verlag Berlin Heidelberg 2001.

[82] Zhaoxia Xie, Manimaran, G., Vittal, V., Phadke, A.G., Centeno, V., “An Information Architecture for Future Power Systems and its Reliability Analysis”, IEEE Trans. On Power Systems, Vol. 17, N0. 3, August 2002.

[83]McHugh, J., “Intrusion and Intrusion Detection”, International Journal of Information Security, Volume 1, Issue 1, Aug 2001, Pages 14 - 35, http://dx.doi.org/10.1007/s102070100001.

[84] Seacord, R.C., Householder, A.D., “A Structured Approach to Classifying Security Vulnerabilities”, Technical Note CMU/SEI-2005-TN-003, January 2005.

[85] Schneier, B., “Attack Trees: Modeling Security Threats”, Dr. Dobb´s Journal, December 1999.

[86] Byres, E.J., Franz, M., Miller, D., “The use of Attack Trees in Assessing Vulnerabilities in SCADA Systems”.

[87] Moore, A.P., Ellison, R.J., Linger, R.C., “Attack Modelling for Information Security and Survivability”, CMU/SEI-2001-TN-001, Carnegie Mellon University, March, 2001.

[88] Mauw, S., Oostdijk, M., “Foundations of Attack Trees”, Proceedings of 8th International Conference on Information Security and Cryptology”, Lectures Notes in Computer Sciences, 2005.

[89] Howard, D.,J., “An analysis of Security Incidents on the Internet 1989-1995”, PhD Thesis, Carnegie Mellon University, 1997, http://www.cert.org/research/JHThesis.

[90] Lundin, E., Jonsson, E. “Survey of Intrusion Detection Research”, Technical Report No. 02-04, Department of Computer Engineering, Chalmers Univeristy of Technology, Götebrog, Sweden, http://citeseer.ist.psu.edu/lundin02survey.html.

[91] Axelsson, S. “Intrusion Detection Systems: A Survey and Taxonomy”, Department of Computer Engineering, Chalmers Univeristy of Technology, Götebrog, Sweden, March, 2000, http://www.cs.plu.edu/courses/CompSec/arts/taxonomy.pdf.

[92] Bace,R., Mell, P. “Intrusion Detection Systems”, NIST Special Publication on Intrusion Detection System, http://csrc.nist.gov/publication/nistpubs/800-31/sp800-31.pdf.

[93] ITL Bulletin, National Institute of Standards and Technology, US Department of Commerce, January, 2007.

[94] ITL Bulletin, National Institute of Standards and Technology, US Department of Commerce, November, 1999.

[95] Kemmerer, R., Vigna,G., “Intrusion Detection: a Brief History and Overview”, Computer, Vol. 35, No. 4, pp. 27-30, April, 2002.

[96] Denning, D., “An Intrusion –Detection Model”, IEEE Trans. On Software Engineering, Vol. SE-13, No. 2, pp. 222-232, Februry, 1987.

[97] Lunt,T., Tamaru,T., Gilham,F., Jagannathan,R., Neumann,P., Javitz,H., Valdes,A., Garvey,T., “A Real Time Intrusion Detection Expert System (IDES)”, Final Technical Report, Computer Science Lab., SRI International, Menlo Park,, California, Feb., 1992

[98] Kumar, S., Spafford, E.H., “A Software Architecture to Support Misuse Intrusion Detection”, Proc. Of the 18th National Information Security Conference, pp. 194-204, 1995.

[99] Ilgun, K., Kemmerer, R.A., Porras, P.A., “State Transition Analysis: A Rule-Based Intrusion Detection Approach”, IEEE Trans. On Software Engineering”, Vol. 21, No. 3, pp. 181-199, 1995.

[100] J. Beale, Caswell (Editor) “Snort 2.1 Intrusion Detection” (2nd Edition), Syngress, 2004.

[101] Bace,R., Mell, P. “Intrusion Detection Systems”, NIST Special Publication on Intrusion Detection System, http://csrc.nist.gov/publication/nistpubs/800-31/sp800-31.pdf.

[102] Porras,P.A., Neumann, P.G., “EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances”, Proc. National Information Systems Security Confrenece, Baltimore, MD, Oct. 1997.

[103] Sarasamma, S.T., Qiuming, A.Zhu, Huff, J., “Hierarchical Kohonenen Net for Anomaly Detection in Network Security”, IEEE Trans. On System, Man, and Cybernetics – Part B, Cybernetics, Vol. 35, No.2, April 2005.

[104] Forrest, S., Hofmeyer, S.A., Somayaji, A., Longstaff, T.A., “A Sense of Self for Unix Process”, Proc. 1996 IEEE Symp. on Security and Privacy, pp. 120-128, 06-08 May 1996, Oakland,CA.IEEE Computer Security Press, Los Alamitos, CA.

[105] Cansian, A.M., “Desenvolvimento de um Sistema Adaptativo de Detecção de Intrusos em Redes de Computadores”, PhD Thesis, Instituto de Física de São Carlos, USP, São Carlos, SP, 1997.

[106] Denning, D. “An Intrusion Detection Model”, Proceedings of the 1986 IEEE Symposium on Security and Privacy, IEEE Press, pp 119–131.

[107] Manikopoulos, C., Papavassiliou,S., “Network Intrusion and Fault Detection: A Statistical Anomaly Approach”, IEEE Communication Magazine, Vol. 40, nO. 10, pp. 76-82, Oct 2002.

[108] Fink, G., C.Ko, Levitt,K., “Automated Detection of Vulnerabilities in privileged Programs by Execution Monitoring”, Proc. Of the 10th Annual Computer Security Apps. Conf. , pp. 134-144, December 5-9, 1994.

[109] Mukkamala, S., Janoski, G., Sung, A., “Intrusion Detection Using Neural Networks and Support Vector Machines”, Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on, Vol. 2, pp 1702-1707, May 2002, Honolulu, HI, USA.

[110] Knowledge Discovery and Data Mining, disponível online em http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[111] Xiangyang Li, Nong Ye, “A Supervised Clustering and Classification Algorithm for Mining Data with Mixed Variables”, IEEE Trans. On Systems, Man, and Cybernetics, Part a: Systems and Humans, Vol. 36, No. 2, March 2006.

[112] Yu, B., Byres, E., Howey, C., “Monitoring Controller's "DNA Sequence for System Security”, ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society, Houston, September 2001.

[113] Scambray, J., McClure, S., Kurtz, G., “Hacking Exposed, Second Edition”, Osborne/MCGraw-Hill, USA, 2001.

[114] Wei Wang, Battiti, R., "Identifying Intrusions in Computer Networks with Principal Component Analysis". Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006), IEEE press society, pp. 270-277, April, 20-22nd, Vienna, Austria.

[115] Dong Song, Heywood, M.I., Zincir-Heywood, A. Nur, “Training Genetic Programming on Half a Million Patterns: An Example from Anomaly Detection”, IEEE Trans. On Evolutionary Computation, Vol. 9, No. 3, June 2005.

[116] Peddabachigari, S., Abraham, A., Grosan, C., Thomas, J., “Modeling Intrusion Detection System using Hibrid Intelligent Systems”, doi:10.1016/J.JNCA.2005.06.03, Elsevier Ltd., 2005.

[117] Holbert, K.E., Mishra, A., Mili, L., “Intrusion Detection Through SCADA Systems Using Fuzzy Logic-Based State Estimation“, International Journal of Critical Infrastructures, Vol. 3, No. 1-2, 2007, pp 58-87.

[118] Mé, Ludovic, Michel, Cédric, “Intrusion Detection: A bibliography”, SUPÉLEC, France, 2001.

[119]Grahan, J. H., Patel, S.,“Security Considerations in SCADA Communications Protocol”, Technical Report TR-ISRL-040-01, Intelligent Systems Research Laboratory, Department of Computer Engineering and Computer Science, Univerisity of Louisville, EUA, September 2003.

[120] McHugh, J., Christie, A., Allen, J., “The Role of Intrusion Detection Systems“, IEEE Software, Vol. 17, Issue 5, Sep./Oct. 2000, pp. 42-51.

[121] Ranum, M., “False Positives: A User´s Guide to Making Sense of IDS Alarms”, ICSA Labs IDSC, February/2003.

[122] Zambon, E., Bolzoni, D., “Network Intrusion Detection Systems: False Positive Reduction Through Anomaly Detection”, http://blackhatnetworks.net/presentations/bh-usa-06/BH-US-06-Zambon.pdf.

[123] Bigham, J., Gamez, D., Ning Lu, “Safeguarding SCADA Systems with Anomaly Detection”, V.Gorodetsky et al.(Eds.):MMM-ACNS 2003, LNCS 2776, pp. 171-182, Springer-Verlag Berlin Heidelberg, 2003.

[124] Bigham, J., Xuan Jin, Gamez, D, Phillips, C., “Hybrid Workflow and Bayesian Networks to Correlate Information in Protection of Large Scale Critical Infrastructures”,

Electronic Notes in Theoretical Computer Science 121 (2005), pp. 87-99, Elsevier B.V., 2005.

[125] Martinelli, M., Tronci, E., Dipoppa, G., Balducelli,C., “Electric Power System Anomaly Detection Using Neural Networks”, M.Gh. Negoita et al. (Eds.), KES 2004, LNAI 3213, pp. 1242-1248, 2004, Springer Verlag Berlin Heidelberg.

[126] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, “IEEE Reliability Test System – 1996”, IEEE Trans. on Power Systems, Vol. 14, No.3, August 1999.

[127] Markou, M., Singh, S., “Novelty Detection: A Review – part 2: Neural Network Based Approaches”, Signal Processing, Vol. 83, 2003.

[128] Japkowicz, N., Myers, C., Gluck, M., “A Novelty Detection Approach to Classification”, Proceedings of the 14th International Conference on Artificial Intelligence”, 20-25 August 1995, pp. 518-523, Montreal, CA.

[129] Conte de Leon, D., Alves-Foss, J., Krings, A., Oman, P., “Modeling Complex Control Systems to Identify remotely Accessible Devices Vulnerable to Cyber Attack”, ACM Workshop on Scientific Aspects of Cyber Terrorism – SACT, Washington DC, November, 2002.

[130] Lee, W., Stolfo, S. J., Chan, K. Philip, Eskin, E., Wei Fan, Miller, M., Hershkop, Junxin Zhang, “Real Time Data Mining-Based Intrusion Detection”, Proceedings of DISCEX II, June 2001.

[131] Haines, J. W., Lippmann, R. P., Fried, D. J., Zissman, M. A., Tran E., and Boswell, S. B., 1999 DARPA Intrusion Detection Evaluation: Design and Procedures, MIT Lincoln Laboratory Technical Report, TR-1062, Lexington, MA, 26 February 2001.

[132]Northcutt, S., Novak, J., “Network Intrusion Detection – An Analyst´s Handbook”, 2nd Edition, New Riders Publishing, EUA, September, 2000.

[133] Allen,J., Christie,A., Fithen, W., McHugh, J., Pickel, J., Stoner, E., “State of the Practice of Intrusion Detection Technologies”, Technical Report CMU/SEI-99-TR-028 ESC 99-028, Software Engineering Institute, Carnegie Melon University, January, 2000.

[134] Rossi, R. – “Classificador Hierárquico Sistêmico para Redes Elétricas de Alta Tensão”, Tese de Doutorado, EFEI, 2000.

[135] Lambert Torres, G., Rossi, R., Alves da Silva, A.P., Jardini, J.A. & Quintana, V.H. - “Power System Security Analysis based on Rough Classification”, Rough-Fuzzy Hybridization: New Trend in Decision Making, por S.K. Pal & A. Skowron, Springer-Verlag Co., ISBN 981-4021-00-8, pp. 263-274, 1999.

[136] Pawlak, Z. - "Rough Sets", International Journal of Information and Computer Sciences Vol. 11, pp. 341-356, 1982.

[137] Pawlak, Z. - "Rough Sets - Theoretical Aspects of Reasoning about Data", Klumer Academic Publishers, 1991.

[138] Baigent, D., Adamiak, M. e Mackienwicz, R., ”IEC 61850 Communication Networks and Systems in Substations: An Overview for Users”.

[139] Curtis, K., DNP3 Primer, Revision A, 20 March 2005, DNP User´s Group, http://www.dnp.org

[140] Wood, A.J., Wollenberg, B.F., “Power Generation Operation and Control”, 2nd Edition, John Wiley & Sons, Inc., 1996.

[141] Moreira, E. M., “Estimação de Estados em Sistemas Elétricos de Potência: Programa para Análise e Atualização das Características Qualitativas do Conjunto de Medidas”, Tese de Mestrado, EESC-USP, São Carlos, SP, 2006.

[142] Medrano Castilho, M.R., “Estimador de Estado e Parâmetros de Linha de Transmissão Baseado nas Equações Normais”, Tese de Mestrado, EESC-USP, São Carlos, SP, 2006.

[143] Xuan Jin, Bigham, J., Rodaway, J., Gamez,D., Phillips, C., “Anomaly Detection in Electricity Cyber Infrastrucuture”, Proceedings of CNIP, 2006, http://www.davidgamez.eu/pages/publications.html

Anexos

A) Simulação da Aplicação do Conjunto de Regras – Caso 1

A.1) Programa fonte em FORTRAN

```
      INTEGER a(100),n,SAIDA
      REAL b(100),c(100),d(100)
C
      OPEN(UNIT=5,FILE="dados.txt",STATUS="old")
      READ(5,*)N
      DO I=1,N
        READ(5,*)A(I),B(I),C(I),D(I)
      END DO
C
      DO I=1,N
      IF(C(I).GT.60) then
         SAIDA=1
      else IF(D(I).GT.1.05) then
         SAIDA=1
      else IF(C(I).LE.40) then
         SAIDA=1
      else IF(C(I).GT.40.AND.C(I).LE.60.AND.D(I).GT.0.95.AND.D(I)
     *.LE.1.05) then
         SAIDA=0
      else IF(C(I).GT.40.AND.C(I).LE.60.AND.D(I).LE.0.95) then
         SAIDA=0
      endif
C
      WRITE(*,10)A(I),B(I),c(I),D(I),SAIDA
10    FORMAT(i3,3F7.2,I5)
      END DO
      STOP
      END
```

A.2) Resultados da Simulação

A.2.1) Usando a Base de Dados Original

```
  0  57.00  82.00   1.07    1
  0  37.00  32.00   0.97    1
  1   0.00  87.00   0.95    1
  1  72.00  31.00   1.07    1
  0  28.00  39.00   1.02    1
  0  42.00  82.00   1.07    1
  0  52.00  59.00   1.01    0
  1  62.00  67.00   1.04    1
  0  57.00  45.00   0.99    0
  0  45.00  58.00   1.00    0 ----------→1.09
  0  32.00  57.00   0.94    0
  0   0.00  57.00   1.08    1
  1  58.00  87.00   1.03    1
  0  58.00  56.00   1.07    1-------------->0.90
  0  25.00  57.00   1.03    0
  0  56.00  54.00   1.08    1------------→0.90
  1  59.00  72.00   1.08    1
  0  32.00   0.00   0.93    1
  0  32.00  45.00   0.94    0
  1  72.00  67.00   0.96    1
  0  57.00  45.00   1.01    0
  0  32.00  45.00   0.94    0
  0  29.00  43.00   1.08    1
  1   0.00  72.00   0.95    1
  1  57.00  79.00   1.07    1
```

```
  0  31.00  43.00   0.99    0
  0  32.00  42.00   0.94    0
  0  17.00  32.00   0.92    1
  0  23.00  22.00   1.00    1
  0  23.00  57.00   0.91    0
```

Obs.: Considera-se o resultado para saída S = 0 para NORMAL e S=1 para estado ANORMAL

A.2.2) Usando a Base de Dados Corrompida

```
  0  57.00  82.00   1.07    1
  0  37.00  32.00   0.97    1
  1   0.00  87.00   0.95    1
  1  72.00  31.00   1.07    1
  0  28.00  39.00   1.02    1
  0  42.00  82.00   1.07    1
  0  52.00  59.00   1.01    0
  1  62.00  67.00   1.04    1
  0  57.00  45.00   0.99    0
  0  45.00  58.00   1.09    1
  0  32.00  57.00   0.94    0
  0   0.00  57.00   1.08    1
  1  58.00  87.00   1.03    1
  0  58.00  56.00   0.90    0
  0  25.00  57.00   1.03    0
  0  56.00  54.00   0.90    0
  1  59.00  72.00   1.08    1
  0  32.00   0.00   0.93    1
  0  32.00  45.00   0.94    0
  1  72.00  67.00   0.96    1
  0  57.00  45.00   1.01    0
  0  32.00  45.00   0.94    0
  0  29.00  43.00   1.08    1
  1   0.00  72.00   0.95    1
  1  57.00  79.00   1.07    1
  0  31.00  43.00   0.99    0
  0  32.00  42.00   0.94    0
  0  17.00  32.00   0.92    1
  0  23.00  22.00   1.00    1
  0  23.00  57.00   0.91    0
```

Obs.: Considera-se o resultado para saída S = 0 para NORMAL e S=1 para estado ANORMAL

B) Simulação da Aplicação do Conjunto de Regras – Caso 2

B.1) Programa fonte em FORTRAN 95

```
      integer a(100),n,SAIDA
      real b(100),c(100),d(100)
C
      OPEN(UNIT=5,FILE="dados.txt",STATUS="old")
      READ(5,*)N
      DO I=1,N
        READ(5,*)A(I),B(I),C(I),D(I)
      END DO
C
      DO I=1,N
      IF(A(I).EQ.0.AND.C(I).GT.60) then
         SAIDA=2
      else IF(A(I).EQ.0.AND.D(I).GT.1.05) then
         SAIDA=2
```

```
      else IF(A(I).EQ.0.AND.C(I).LE.40) then
         SAIDA=1
      else IF(C(I).LE.40.AND.D(I).GT.0.95.AND.D(I).LE.1.05) then
         SAIDA=1
      else IF(A(I).EQ.1) then
         SAIDA=3
      else IF(C(I).GT.60.AND.D(I).GT.0.95.AND.D(I).LE.1.05) then
         SAIDA=3
      else IF(C(I).LE.40.AND.D(I).GT.1.05) then
         SAIDA=3
      else IF(C(I).GT.40.AND.C(I).LE.60.AND.D(I).GT.0.95.AND.
     *D(I).LE.1.05) then
         SAIDA=0
      else IF(C(I).GT.40.AND.C(I).LE.60.AND.D(I).LE.0.95)then
         SAIDA=0
      else IF(C(I).GT.40.AND.C(I).LE.60.AND.D(I).GT.1.05) then
         SAIDA=2
      else IF(C(I).LE.40.AND.D(I).LE.0.95) then
         SAIDA=1
      endif
C
      WRITE(*,10)A(I),B(I),c(I),D(I),SAIDA
10    FORMAT(i3,3F7.2,I5)
      END DO
      STOP
      END
```

B.2) Resultados da Simulação

B.2.1) Usando a Base de Dados Original

```
  0  57.00  82.00   1.07    2
  0  37.00  32.00   0.97    1
  1   0.00  87.00   0.95    3
  1  72.00  31.00   1.07    3
  0  28.00  39.00   1.02    1
  0  42.00  82.00   1.07    2
  0  52.00  59.00   1.01    0
  1  62.00  67.00   1.04    3
  0  57.00  45.00   0.99    0
  0  45.00  58.00   1.00    0----------------→1.09
  0  32.00  57.00   0.94    0
  0   0.00  57.00   1.08    2
  1  58.00  87.00   1.03    3
  0  58.00  56.00   1.07    2----------------->0.90
  0  25.00  57.00   1.03    0
  0  56.00  54.00   1.08    2----------------->0.90
  1  59.00  72.00   1.08    3
  0  32.00   0.00   0.93    1
  0  32.00  45.00   0.94    0
  1  72.00  67.00   0.96    3
  0  57.00  45.00   1.01    0
  0  32.00  45.00   0.94    0
  0  29.00  43.00   1.08    2
  1   0.00  72.00   0.95    3
  1  57.00  79.00   1.07    3
  0  31.00  43.00   0.99    0
  0  32.00  42.00   0.94    0
  0  17.00  32.00   0.92    1
  0  23.00  22.00   1.00    1
  0  23.00  57.00   0.91    0
```

B.2.2) Usando a Base de Dados Corrompida

```
  0  57.00  82.00   1.07    2
  0  37.00  32.00   0.97    1
  1   0.00  87.00   0.95    3
  1  72.00  31.00   1.07    3
  0  28.00  39.00   1.02    1
```

```
  0  42.00  82.00   1.07    2
  0  52.00  59.00   1.01    0
  1  62.00  67.00   1.04    3
  0  57.00  45.00   0.99    0
  0  45.00  58.00   1.09    2
  0  32.00  57.00   0.94    0
  0   0.00  57.00   1.08    2
  1  58.00  87.00   1.03    3
  0  58.00  56.00   0.90    0
  0  25.00  57.00   1.03    0
  0  56.00  54.00   0.90    0
  1  59.00  72.00   1.08    3
  0  32.00   0.00   0.93    1
  0  32.00  45.00   0.94    0
  1  72.00  67.00   0.96    3
  0  57.00  45.00   1.01    0
  0  32.00  45.00   0.94    0
  0  29.00  43.00   1.08    2
  1   0.00  72.00   0.95    3
  1  57.00  79.00   1.07    3
  0  31.00  43.00   0.99    0
  0  32.00  42.00   0.94    0
  0  17.00  32.00   0.92    1
  0  23.00  22.00   1.00    1
  0  23.00  57.00   0.91    0
```

C) Caso Teste 1 Usando Sistema de 6 Barras

C.1) Código fonte em Matlab para Implementar Detector de Anomalias – Caso Teste 1

```
%=====================================================
%
% Módulo para Detecção de Anomalias
% Faixa de Operação 0.5 até 0.90
%
%=====================================================
nome=input('Entre com nome do arquivo de dados: ');
fid=fopen(nome, 'r');
nentradas=input('Entre com número de entradas: ');
lista=fscanf(fid,'%f');
fclose(fid);
lista=reshape(lista,57,nentradas)';
for i=1:nentradas
   if (lista(i,8)>=-0.6) & (lista(i,8)<-0.3) & (lista(i,12)>=-0.9) & (lista(i,12)<-0.6)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.9) & (lista(i,8)<-0.6) & (lista(i,12)>=-0.6) & (lista(i,12)<-
0.3)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.6) & (lista(i,8)<-0.3) & (lista(i,12)>=-0.6) & (lista(i,12)<-
0.3)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.9) & (lista(i,8)<-0.6) & (lista(i,12)>=-0.9) & (lista(i,12)<-
0.6)
      resultado(i,1)=0;
   elseif (lista(i,8)>=0.3) & (lista(i,8)<0.6)
      resultado(i,1)=1;
   elseif (lista(i,12)>=0.6) & (lista(i,12)<0.95)
      resultado(i,1)=1;
   elseif (lista(i,12)>=0.3) & (lista(i,12)<0.6)
      resultado(i,1)=1;
   elseif (lista(i,8)>=0.6) & (lista(i,8)<0.95)
      resultado(i,1)=1;
   else resultado(i,1)=2;
   end;
end;
      for i=1:nentradas
         if resultado(i,1) == 0
            saida='NORMAL';
```

```
        end;
        if resultado(i,1) == 1
           saida='ANORMAL';
        end;
        if resultado(i,1)== 2
            saida='FORA DE FAIXA';
        end;
        fprintf(1,'Entrada: %+8.3f %+8.3f   Resultado:
%s\n',lista(i,8),lista(i,12),saida);
      end;
```

C.2) Caso Teste 1

```
1.0500   1.0366   0.2064   0.5000   0.9943   0.6000   0.6000  -0.6300  -0.7000  -0.7000
-0.7000  -0.7300  -0.7000   0.2770  -0.1500   0.4082   0.2051   0.3514   0.1513  -0.2685
0.1228   0.0237  -0.0057   0.3022   0.4726   0.1622   0.1898   0.2804   0.2149  -0.0237
-0.0596   0.1771   0.1647   0.4465   0.4949  -0.3983  -0.2071  -0.2875  -0.4639   0.0558
-0.0290  -0.3400  -0.1700  -0.1557  -0.2115  -0.1696  -0.1993  -0.0551  -0.0469   0.0204
-0.0723  -0.2717  -0.2418  -0.4382  -0.4736  -0.0202   0.0154


  1.0500   1.0385   0.2105   0.5000   1.0000   0.6000   0.6000  -0.5300  -0.7000  -
0.7000  -0.7000  -0.8300  -0.7000   0.2879  -0.1471   0.3865   0.2008   0.3641   0.1568
-0.2789   0.1210   0.0462  -0.0008   0.2400   0.4707   0.1678   0.1904   0.3249   0.2187
-0.0460  -0.0639   0.1636   0.1641   0.4824   0.4998  -0.3775  -0.2064  -0.2269  -0.4652
0.0744  -0.0284  -0.3518  -0.1723  -0.1611  -0.2113  -0.1566  -0.1994  -0.0732  -0.0464
0.0428  -0.0706  -0.3144  -0.2400  -0.4732  -0.4745  -0.0424   0.0145

  1.0500   1.0571   0.2199   0.5000   0.9792   0.6000   0.6000  -0.7700  -0.7000  -
0.7000  -0.7000  -0.6100  -0.7000   0.2714  -0.1476   0.4454   0.2181   0.3403   0.1495
-0.2633   0.1197  -0.0034  -0.0115   0.3849   0.4717   0.1549   0.1882   0.2269   0.2110
0.0034  -0.0543   0.1928   0.1646   0.4038   0.4897  -0.4338  -0.2131  -0.3676  -0.4579
0.0313  -0.0290  -0.3294  -0.1705  -0.1487  -0.2107  -0.1847  -0.1981  -0.0311  -0.0475
-0.0060  -0.0732  -0.2200  -0.2434  -0.3962  -0.4725   0.0062   0.0159

  1.0500   0.8981   0.2511   0.5000   0.9186   0.6000   0.6000  -0.7100  -0.7000  -
0.7000  -0.7000  -0.5200  -0.7000   0.2141  -0.1227   0.3840   0.2217   0.3000   0.1521
-0.2090   0.0888  -0.0202  -0.0174   0.3835   0.4577   0.1553   0.1833   0.1905   0.2062
0.0203  -0.0484   0.2082   0.1619   0.3715   0.4865  -0.3746  -0.2257  -0.3669  -0.4452
0.0315  -0.0290  -0.2910  -0.1800  -0.1492  -0.2064  -0.1995  -0.1944  -0.0313  -0.0477
-0.0290  -0.0715  -0.1847  -0.2419  -0.3645  -0.4722   0.0292   0.0141

  1.0500   1.0844   0.2353   0.4999   1.0003   0.6000   0.6000  -0.4500  -0.7000  -
0.7000  -0.7000  -0.9499  -0.7000   0.3150  -0.1387   0.3822   0.2052   0.3872   0.1687
-0.3048   0.1153   0.0725   0.0055   0.1809   0.4649   0.1734   0.1904   0.3780   0.2243
-0.0722  -0.0687   0.1466   0.1625   0.5256   0.5062  -0.3732  -0.2110  -0.1690  -0.4618
0.0923  -0.0271  -0.3733  -0.1780  -0.1665  -0.2103  -0.1401  -0.1986  -0.0905  -0.0460
0.0705  -0.0671  -0.3648  -0.2375  -0.5154  -0.4753  -0.0698   0.0128

  1.0500   1.3037   0.2628   0.4998   1.0007   0.5999   0.6000  -0.8299  -0.7000  -
0.6999  -0.7000  -0.7799  -0.7000   0.3659  -0.1467   0.5322   0.2408   0.4056   0.1687
-0.3524   0.1300   0.0304  -0.0031   0.3673   0.4676   0.1569   0.1890   0.2976   0.2172
-0.0303  -0.0611   0.1652   0.1637   0.4650   0.4974  -0.5162  -0.2181  -0.3505  -0.4545
0.0369  -0.0273  -0.3907  -0.1739  -0.1506  -0.2103  -0.1581  -0.1983  -0.0365  -0.0477
0.0361  -0.0698  -0.2880  -0.2409  -0.4561  -0.4732  -0.0357   0.0141

  1.0500   1.1243   0.2330   0.4999   1.0002   0.6000   0.6000  -0.5600  -0.7000  -
0.7000  -0.7000  -0.8800  -0.7000   0.3200  -0.1434   0.4186   0.2113   0.3857   0.1652
-0.3094   0.1208   0.0560   0.0018   0.2395   0.4666   0.1681   0.1900   0.3457   0.2210
-0.0558  -0.0657   0.1553   0.1632   0.5005   0.5024  -0.4082  -0.2112  -0.2265  -0.4612
0.0747  -0.0276  -0.3720  -0.1752  -0.1614  -0.2106  -0.1485  -0.1988  -0.0735  -0.0466
0.0554  -0.0688  -0.3341  -0.2389  -0.4909  -0.4746  -0.0549   0.0136

  1.0500   0.7823   0.2612   0.5000   0.8920   0.6000   0.6000  -0.5600  -0.7000  -
0.7000  -0.7000  -0.5600  -0.7000   0.1828  -0.1088   0.3157   0.2148   0.2838   0.1552
-0.1791   0.0721  -0.0091  -0.0170   0.3166   0.4500   0.1613   0.1814   0.2103   0.2055
0.0091  -0.0489   0.2052   0.1604   0.3857   0.4885  -0.3087  -0.2283  -0.3025  -0.4425
0.0511  -0.0293  -0.2754  -0.1853  -0.1551  -0.2042  -0.1967  -0.1933  -0.0506  -0.0471
-0.0222  -0.0701  -0.2041  -0.2398  -0.3784  -0.4729   0.0225   0.0127

  1.0500   1.2193   0.2505   0.4999   1.0005   0.5999   0.6000  -0.6699  -0.7000  -
0.6999  -0.7000  -0.8599  -0.7000   0.3477  -0.1437   0.4713   0.2252   0.4003   0.1691
```

-0.3354 0.1245 0.0498 0.0008 0.2864 0.4654 0.1641 0.1895 0.3350 0.2203
-0.0497 -0.0646 0.1561 0.1631 0.4935 0.5015 -0.4585 -0.2152 -0.2722 -0.4576
0.0608 -0.0273 -0.3857 -0.1755 -0.1575 -0.2103 -0.1493 -0.1984 -0.0600 -0.0472
0.0525 -0.0686 -0.3238 -0.2393 -0.4840 -0.4742 -0.0521 0.0135

1.0500 1.0447 0.2050 0.5000 1.0000 0.6000 0.6000 **-0.6010** -0.7000 -
0.7000 -0.7000 **-0.7661** -0.7000 0.2831 -0.1508 0.4042 0.2031 0.3573 0.1527
-0.2743 0.1242 0.0317 -0.0038 0.2824 0.4730 0.1639 0.1903 0.2963 0.2163
-0.0316 -0.0613 0.1721 0.1647 0.4595 0.4966 -0.3945 -0.2059 -0.2682 -0.4653
0.0617 -0.0288 -0.3456 -0.1700 -0.1574 -0.2117 -0.1648 -0.1996 -0.0609 -0.0467
0.0286 -0.0719 -0.2869 -0.2414 -0.4508 -0.4739 -0.0283 0.0153

1.0500 1.0366 0.2064 0.5000 0.9943 0.6000 0.6000 **+0.6300** -0.7000 -
0.7000 -0.7000 **-0.7300** -0.7000 0.2770 -0.1500 0.4082 0.2051 0.3514 0.1513
-0.2685 0.1228 0.0237 -0.0057 0.3022 0.4726 0.1622 0.1898 0.2804 0.2149
-0.0237 -0.0596 0.1771 0.1647 0.4465 0.4949 -0.3983 -0.2071 -0.2875 -0.4639
0.0558 -0.0290 -0.3400 -0.1700 -0.1557 -0.2115 -0.1696 -0.1993 -0.0551 -0.0469
0.0204 -0.0723 -0.2717 -0.2418 -0.4382 -0.4736 -0.0202 0.0154

1.0500 1.0385 0.2105 0.5000 1.0000 0.6000 0.6000 **-0.5300** -0.7000 -
0.7000 -0.7000 **+0.8300** -0.7000 0.2879 -0.1471 0.3865 0.2008 0.3641 0.1568
-0.2789 0.1210 0.0462 -0.0008 0.2400 0.4707 0.1678 0.1904 0.3249 0.2187
-0.0460 -0.0639 0.1636 0.1641 0.4824 0.4998 -0.3775 -0.2064 -0.2269 -0.4652
0.0744 -0.0284 -0.3518 -0.1723 -0.1611 -0.2113 -0.1566 -0.1994 -0.0732 -0.0464
0.0428 -0.0706 -0.3144 -0.2400 -0.4732 -0.4745 -0.0424 0.0145

1.0500 1.0571 0.2199 0.5000 0.9792 0.6000 0.6000 **+0.7700** -0.7000 -
0.7000 -0.7000 **+0.6100** -0.7000 0.2714 -0.1476 0.4454 0.2181 0.3403 0.1495
-0.2633 0.1197 -0.0034 -0.0115 0.3849 0.4717 0.1549 0.1882 0.2269 0.2110
0.0034 -0.0543 0.1928 0.1646 0.4038 0.4897 -0.4338 -0.2131 -0.3676 -0.4579
0.0313 -0.0290 -0.3294 -0.1705 -0.1487 -0.2107 -0.1847 -0.1981 -0.0311 -0.0475
-0.0060 -0.0732 -0.2200 -0.2434 -0.3962 -0.4725 0.0062 0.0159

1.0500 0.8981 0.2511 0.5000 0.9186 0.6000 0.6000 **-0.7100** -0.7000 -
0.7000 -0.7000 **+0.5200** -0.7000 0.2141 -0.1227 0.3840 0.2217 0.3000 0.1521
-0.2090 0.0888 -0.0202 -0.0174 0.3835 0.4577 0.1553 0.1833 0.1905 0.2062
0.0203 -0.0484 0.2082 0.1619 0.3715 0.4865 -0.3746 -0.2257 -0.3669 -0.4452
0.0315 -0.0290 -0.2910 -0.1800 -0.1492 -0.2064 -0.1995 -0.1944 -0.0313 -0.0477
-0.0290 -0.0715 -0.1847 -0.2419 -0.3645 -0.4722 0.0292 0.0141

1.0500 1.0844 0.2353 0.4999 1.0003 0.6000 0.6000 **+0.4500** -0.7000 -
0.7000 -0.7000 **-0.9499** -0.7000 0.3150 -0.1387 0.3822 0.2052 0.3872 0.1687
-0.3048 0.1153 0.0725 0.0055 0.1809 0.4649 0.1734 0.1904 0.3780 0.2243
-0.0722 -0.0687 0.1466 0.1625 0.5256 0.5062 -0.3732 -0.2110 -0.1690 -0.4618
0.0923 -0.0271 -0.3733 -0.1780 -0.1665 -0.2103 -0.1401 -0.1986 -0.0905 -0.0460
0.0705 -0.0671 -0.3648 -0.2375 -0.5154 -0.4753 -0.0698 0.0128

1.0500 1.3037 0.2628 0.4998 1.0007 0.5999 0.6000 **-0.8299** -0.7000 -
0.6999 -0.7000 **+0.7799** -0.7000 0.3659 -0.1467 0.5322 0.2408 0.4056 0.1687
-0.3524 0.1300 0.0304 -0.0031 0.3673 0.4676 0.1569 0.1890 0.2976 0.2172
-0.0303 -0.0611 0.1652 0.1637 0.4650 0.4974 -0.5162 -0.2181 -0.3505 -0.4545
0.0369 -0.0273 -0.3907 -0.1739 -0.1506 -0.2103 -0.1581 -0.1983 -0.0365 -0.0477
0.0361 -0.0698 -0.2880 -0.2409 -0.4561 -0.4732 -0.0357 0.0141

1.0500 1.1243 0.2330 0.4999 1.0002 0.6000 0.6000 **+0.5600** -0.7000 -
0.7000 -0.7000 **+0.8800** -0.7000 0.3200 -0.1434 0.4186 0.2113 0.3857 0.1652
-0.3094 0.1208 0.0560 0.0018 0.2395 0.4666 0.1681 0.1900 0.3457 0.2210
-0.0558 -0.0657 0.1553 0.1632 0.5005 0.5024 -0.4082 -0.2112 -0.2265 -0.4612
0.0747 -0.0276 -0.3720 -0.1752 -0.1614 -0.2106 -0.1485 -0.1988 -0.0735 -0.0466
0.0554 -0.0688 -0.3341 -0.2389 -0.4909 -0.4746 -0.0549 0.0136

1.0500 0.7823 0.2612 0.5000 0.8920 0.6000 0.6000 **+0.5600** -0.7000 -
0.7000 -0.7000 **-0.5600** -0.7000 0.1828 -0.1088 0.3157 0.2148 0.2838 0.1552
-0.1791 0.0721 -0.0091 -0.0170 0.3166 0.4500 0.1613 0.1814 0.2103 0.2055
0.0091 -0.0489 0.2052 0.1604 0.3857 0.4885 -0.3087 -0.2283 -0.3025 -0.4425
0.0511 -0.0293 -0.2754 -0.1853 -0.1551 -0.2042 -0.1967 -0.1933 -0.0506 -0.0471
-0.0222 -0.0701 -0.2041 -0.2398 -0.3784 -0.4729 0.0225 0.0127

1.0500 1.2193 0.2505 0.4999 1.0005 0.5999 0.6000 **-0.6699** -0.7000 -
0.6999 -0.7000 **+0.8599** -0.7000 0.3477 -0.1437 0.4713 0.2252 0.4003 0.1691
-0.3354 0.1245 0.0498 0.0008 0.2864 0.4654 0.1641 0.1895 0.3350 0.2203
-0.0497 -0.0646 0.1561 0.1631 0.4935 0.5015 -0.4585 -0.2152 -0.2722 -0.4576
0.0608 -0.0273 -0.3857 -0.1755 -0.1575 -0.2103 -0.1493 -0.1984 -0.0600 -0.0472
0.0525 -0.0686 -0.3238 -0.2393 -0.4840 -0.4742 -0.0521 0.0135

```
  1.0500    1.0447    0.2050    0.5000    1.0000    0.6000    0.6000   -0.6010   -0.7000   -
0.7000   -0.7000   +0.7661   -0.7000    0.2831   -0.1508    0.4042    0.2031    0.3573    0.1527
-0.2743    0.1242    0.0317   -0.0038    0.2824    0.4730    0.1639    0.1903    0.2963    0.2163
-0.0316   -0.0613    0.1721    0.1647    0.4595    0.4966   -0.3945   -0.2059   -0.2682   -0.4653
0.0617   -0.0288   -0.3456   -0.1700   -0.1574   -0.2117   -0.1648   -0.1996   -0.0609   -0.0467
0.0286   -0.0719   -0.2869   -0.2414   -0.4508   -0.4739   -0.0283    0.0153
```

C.3) Resultado do Caso Teste 1

```
» regrasdb
Entre com nome do arquivo de dados: 'caso_teste.txt'
Entre com número de entradas: 20
Entrada:   -0.630   -0.730   Resultado: NORMAL
Entrada:   -0.530   -0.830   Resultado: NORMAL
Entrada:   -0.770   -0.610   Resultado: NORMAL
Entrada:   -0.710   -0.520   Resultado: NORMAL
Entrada:   -0.450   -0.950   Resultado: FORA DE FAIXA
Entrada:   -0.830   -0.780   Resultado: NORMAL
Entrada:   -0.560   -0.880   Resultado: NORMAL
Entrada:   -0.560   -0.560   Resultado: NORMAL
Entrada:   -0.670   -0.860   Resultado: NORMAL
Entrada:   -0.601   -0.766   Resultado: NORMAL
Entrada:   +0.630   -0.730   Resultado: ANORMAL
Entrada:   -0.530   +0.830   Resultado: ANORMAL
Entrada:   +0.770   +0.610   Resultado: ANORMAL
Entrada:   -0.710   +0.520   Resultado: ANORMAL
Entrada:   +0.450   -0.950   Resultado: ANORMAL
Entrada:   -0.830   +0.780   Resultado: ANORMAL
Entrada:   +0.560   +0.880   Resultado: ANORMAL
Entrada:   +0.560   -0.560   Resultado: ANORMAL
Entrada:   -0.670   +0.860   Resultado: ANORMAL
Entrada:   -0.601   +0.766   Resultado: ANORMAL
```

D) Caso Teste 2 Usando Sistema de 6 Barras

D.1) Código fonte em Matlab para Implementar Detector de Anomalias – Caso Teste 2

```
%=====================================================
%
%Módulo para Detecção de Anomalias
%Faixa de Operação 0.3 até 1.10 - caso 5
%
%=====================================================
nome=input('Entre com nome do arquivo de dados: ');
fid=fopen(nome, 'r');
nentradas=input('Entre com número de entradas: ');
lista=fscanf(fid,'%f');
fclose(fid);
lista=reshape(lista,57,nentradas)';
for i=1:nentradas
   if (lista(i,8)>=-0.7333) & (lista(i,8)<-0.3667) & (lista(i,12)>=-0.7333) &
(lista(i,12)<-0.3667)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-1.1) & (lista(i,8)<-0.7333) & (lista(i,12)>=-0.7333) &
(lista(i,12)<-0.3667)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.7333) & (lista(i,8)<-0.3667) & (lista(i,12)>=-1.1) &
(lista(i,12)<-0.7333)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-1.1) & (lista(i,8)<-0.7333) & (lista(i,12)>=-1.1) &
(lista(i,12)<-0.7333)
      resultado(i,1)=0;
   elseif (lista(i,8)>=0.3667) & (lista(i,8)<0.7333)
      resultado(i,1)=1;
   elseif (lista(i,12)>=0.3667) & (lista(i,12)<0.7333)
```

```
      resultado(i,1)=1;
   elseif (lista(i,8)>=0.7333) & (lista(i,8)<1.101)
      resultado(i,1)=1;
   elseif (lista(i,12)>=0.7333) & (lista(i,8)<1.101)
      resultado(i,1)=1;
   elseif (lista(i,8)>=-0.3667) & (lista(i,8)<0.0) & (lista(i,12)>=-0.7333) &
(lista(i,12)<-0.3667)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.7333) & (lista(i,8)<-0.3667) & (lista(i,12)>=-0.3667) &
(lista(i,12)<0.0)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-0.3667) & (lista(i,8)<0.0) & (lista(i,12)>=-0.3667) &
(lista(i,12)<0.0)
      resultado(i,1)=0;
   elseif (lista(i,8)>=0.0) & (lista(i,8)<0.3667)
      resultado(i,1)=1;
   elseif (lista(i,12)>=0.0) & (lista(i,8)<0.3667)
      resultado(i,1)=1;
   elseif (lista(i,8)>=-0.3667) & (lista(i,8)<0.0) & (lista(i,12)>=-1.1) &
(lista(i,12)<-0.7333)
      resultado(i,1)=0;
   elseif (lista(i,8)>=-1.1) & (lista(i,8)<-0.7333) & (lista(i,12)>=-0.3667) &
(lista(i,12)<0.0)
      resultado(i,1)=0;
   else resultado(i,1)=2;
   end;
end;
      for i=1:nentradas
         if resultado(i,1) == 0
            saida='NORMAL';
         end;
         if resultado(i,1) == 1
            saida='ANORMAL';
         end;
         if resultado(i,1)== 2
               saida='FORA DE FAIXA';
         end;
         fprintf(1,'Entrada: %+8.3f %+8.3f   Resultado:
%s\n',lista(i,8),lista(i,12),saida);
      end;
```

E) Caso Teste Estudo de Tensão

E.1) Exemplo de Arquivo SCADA

```
SIXBUS POWER FLOW SAMPLE SYSTEM
-------------------------------
6
11
LINE    1    2  1.00000E-01  2.00000E-01  2.00000E-02
LINE    1    4  5.00000E-02  2.00000E-01  2.00000E-02
LINE    1    5  8.00000E-02  3.00000E-01  3.00000E-02
LINE    2    3  5.00000E-02  2.50000E-01  3.00000E-02
LINE    2    4  5.00000E-02  1.00000E-01  1.00000E-02
LINE    2    5  1.00000E-01  3.00000E-01  2.00000E-02
LINE    2    6  7.00000E-02  2.00000E-01  2.50000E-02
LINE    3    5  1.20000E-01  2.60000E-01  2.50000E-02
LINE    3    6  2.00000E-02  1.00000E-01  1.00000E-02
LINE    4    5  2.00000E-01  4.00000E-01  4.00000E-02
LINE    5    6  1.00000E-01  3.00000E-01  3.00000E-02
V    1     1.0500000000E+00  1.000E-04
V    4     9.9757488501E-01  1.000E-04
V    6     9.8744382133E-01  1.000E-04
A    1     0.0000000000E+00  1.000E-04
A    4    -3.1603824341E-02  1.000E-04
A    6    -7.2849142749E-02  1.000E-04
I    1     6.5929218705E-01  1.000E-02     2.6187809122E-01  1.000E-02
I    2     5.0000093699E-01  1.000E-02     8.8506883860E-01  1.000E-02
I    3     5.9999839036E-01  1.000E-02     6.0000441548E-01  1.000E-02
I    4    -2.9999998259E-01  1.000E-02    -6.9999995148E-01  1.000E-02
I    5    -6.9999932338E-01  1.000E-02    -7.0000007968E-01  1.000E-02
```

```
I    6    -6.9999855898E-01  1.000E-02    -6.9999986328E-01  1.000E-02
F    1     2      1.5939034534E-01  1.000E-02    -9.8207168545E-02  1.000E-02
F    1     4      2.2113123173E-01  1.000E-02     2.0051432426E-01  1.000E-02
F    1     5      2.7877060998E-01  1.000E-02     1.5957093551E-01  1.000E-02
F    2     1     -1.5655994203E-01  1.000E-02     5.9767975171E-02  1.000E-02
F    2     3      2.4348613909E-02  1.000E-02    -1.1503473486E-02  1.000E-02
F    2     4      1.8481178134E-01  1.000E-02     4.4712634354E-01  1.000E-02
F    2     5      1.7296121869E-01  1.000E-02     1.8132246949E-01  1.000E-02
F    2     6      2.7443926508E-01  1.000E-02     2.0835552389E-01  1.000E-02
F    3     2     -2.4300623625E-02  1.000E-02    -5.4011827979E-02  1.000E-02
F    3     5      1.8880513191E-01  1.000E-02     1.5926827622E-01  1.000E-02
F    3     6      4.3549388208E-01  1.000E-02     4.9474796724E-01  1.000E-02
F    4     1     -2.1666710928E-01  1.000E-02    -2.2461094747E-01  1.000E-02
F    4     2     -1.7374338914E-01  1.000E-02    -4.4596611567E-01  1.000E-02
F    4     5      9.0410515824E-02  1.000E-02    -2.9422888348E-02  1.000E-02
F    5     1     -2.7043860022E-01  1.000E-02    -1.8997137530E-01  1.000E-02
F    5     2     -1.6649628042E-01  1.000E-02    -2.0302463891E-01  1.000E-02
F    5     3     -1.8104665141E-01  1.000E-02    -1.9350050954E-01  1.000E-02
F    5     4     -8.8746077691E-02  1.000E-02    -4.5148429950E-02  1.000E-02
F    5     6      6.7282863581E-03  1.000E-02    -6.8355125973E-02  1.000E-02
F    6     2     -2.6612344131E-01  1.000E-02    -2.3653465994E-01  1.000E-02
F    6     3     -4.2731778627E-01  1.000E-02    -4.7451135879E-01  1.000E-02
F    6     5     -6.5573314019E-03  1.000E-02     1.1046155451E-02  1.000E-02
Q
```

E.2)Módulo de Detecção de Anomalias em Matlb

```
%=====================================================
%
%Módulo para Detecção de Anomalias
%Caso teste : Estudo de Tensão
%Faixa de Operação 0.3pu até 1.8 pu
%
%=====================================================
ncol=input('Entre com número de colunas: ');
nc=ncol;
lista=fscanf(fid,'%f');
fclose(fid);
lista=reshape(lista,nc,nentradas)';
for i=1:nentradas
   if (lista(i,2)>=0.9217) & (lista(i,2)<0.9977) & (lista(i,3)>=0.9071) &
(lista(i,3)<1.0007)
      resultado(i,1)=0;
   elseif (lista(i,2)>=0.8459) & (lista(i,2)<0.9217)
      resultado(i,1)=1;
      elseif (lista(i,3)>=0.8135) & (lista(i,3)<0.9071)
         resultado(i,1)=1;
      elseif (lista(i,2)>=0.77) & (lista(i,2)<0.8459)
      resultado(i,1)=1;
      elseif (lista(i,3)>=0.72) & (lista(i,3)<0.8135)
      resultado(i,1)=1;
   else resultado(i,1)=2;
   end;
end;
      for i=1:nentradas
         if resultado(i,1) == 0
            saida='NORMAL';
         end;
         if resultado(i,1) == 1
            saida='ANORMAL';
         end;
         if resultado(i,1)== 2
               saida='FORA DE FAIXA';
         end;
         fprintf(1,'Entrada: %5d %+8.3f %+8.3f   Resultado:
%s\n',i,lista(i,2),lista(i,3),saida);
      end;
```

E.3)Arquivo de dados do Caso Teste

- 1.0500 0.9941 0.9854 0.8683 0.2252 0.5000 0.9509 0.6000 0.6000 -
  0.4500 -0.7000 -0.7000 -0.7000 -0.7500 -0.7000 0.2276 -0.1287 0.3176
  0.1987 0.3231 0.1551 -0.2219 0.0961 0.0314 -0.0066 0.2291 0.4616
  0.1688 0.1865 0.2925 0.2133 -0.0314 -0.0587 0.1778 0.1623 0.4535
  0.4964 -0.3108 -0.2134 -0.2166 -0.4575 0.0774 -0.0291 -0.3130 -0.1786 -
  0.1623 -0.2080 -0.1704 -0.1971 -0.0762 -0.0460 0.0218 -0.0703 -0.2834 -
  0.2391 -0.4450 -0.4743 -0.0216 0.0134

- 1.0500 0.9 0.85 0.8683 0.2252 0.5000 0.9509 0.6000 0.6000 -
  0.4500 -0.7000 -0.7000 -0.7000 -0.7500 -0.7000 0.2276 -0.1287 0.3176
  0.1987 0.3231 0.1551 -0.2219 0.0961 0.0314 -0.0066 0.2291 0.4616
  0.1688 0.1865 0.2925 0.2133 -0.0314 -0.0587 0.1778 0.1623 0.4535
  0.4964 -0.3108 -0.2134 -0.2166 -0.4575 0.0774 -0.0291 -0.3130 -0.1786 -
  0.1623 -0.2080 -0.1704 -0.1971 -0.0762 -0.0460 0.0218 -0.0703 -0.2834 -
  0.2391 -0.4450 -0.4743 -0.0216 0.0134

- 1.0500 0.9818 0.9602 1.3006 0.2974 0.5000 1.0000 0.6000 0.6000 -
  0.5500 -0.7000 -0.7000 -0.7000 -1.0500 -0.7000 0.3938 -0.1277 0.4683
  0.2346 0.4386 0.1906 -0.3787 0.1143 0.0916 0.0114 0.1949 0.4543
  0.1728 0.1895 0.4194 0.2304 -0.0911 -0.0726 0.1289 0.1603 0.5622
  0.5122 -0.4554 -0.2242 -0.1830 -0.4510 0.0884 -0.0248 -0.4210 -0.1853 -
  0.1659 -0.2086 -0.1230 -0.1966 -0.0868 -0.0472 0.0967 -0.0624 -0.4036 -
  0.2352 -0.5509 -0.4754 -0.0955 0.0106

- 1.0500 0.8818 0.9102 1.3006 0.2974 0.5000 1.0000 0.6000 0.6000 -
  0.5500 -0.7000 -0.7000 -0.7000 -1.0500 -0.7000 0.3938 -0.1277 0.4683
  0.2346 0.4386 0.1906 -0.3787 0.1143 0.0916 0.0114 0.1949 0.4543
  0.1728 0.1895 0.4194 0.2304 -0.0911 -0.0726 0.1289 0.1603 0.5622
  0.5122 -0.4554 -0.2242 -0.1830 -0.4510 0.0884 -0.0248 -0.4210 -0.1853 -
  0.1659 -0.2086 -0.1230 -0.1966 -0.0868 -0.0472 0.0967 -0.0624 -0.4036 -
  0.2352 -0.5509 -0.4754 -0.0955 0.0106

- 1.0500 0.9286 0.9157 2.3602 0.6778 0.4999 1.0000 0.5997 0.6003 -
  1.3999 -0.7000 -0.6999 -0.7000 -1.1497 -0.7000 0.7442 -0.0631 0.9744
  0.4479 0.6416 0.2930 -0.6939 0.1220 0.0975 0.0194 0.5008 0.4331
  0.1485 0.1843 0.4469 0.2413 -0.0969 -0.0751 0.0957 0.1543 0.6009
  0.5211 -0.9213 -0.2749 -0.4783 -0.4068 -0.0003 -0.0184 -0.6040 -0.2106 -
  0.1421 -0.2020 -0.0906 -0.1885 0.0003 -0.0500 0.1364 -0.0489 -0.4279 -
  0.2327 -0.5876 -0.4722 -0.1342 0.0050

- 1.0500 0.8286 0.9057 2.3602 0.6778 0.4999 1.0000 0.5997 0.6003 -
  1.3999 -0.7000 -0.6999 -0.7000 -1.1497 -0.7000 0.7442 -0.0631 0.9744
  0.4479 0.6416 0.2930 -0.6939 0.1220 0.0975 0.0194 0.5008 0.4331
  0.1485 0.1843 0.4469 0.2413 -0.0969 -0.0751 0.0957 0.1543 0.6009
  0.5211 -0.9213 -0.2749 -0.4783 -0.4068 -0.0003 -0.0184 -0.6040 -0.2106 -
  0.1421 -0.2020 -0.0906 -0.1885 0.0003 -0.0500 0.1364 -0.0489 -0.4279 -
  0.2327 -0.5876 -0.4722 -0.1342 0.0050

- 1.0500 0.9217 0.9258 2.4168 0.6873 0.4999 1.0000 0.5998 0.6002 -
  1.6499 -0.7000 -0.6999 -0.7000 -0.9498 -0.7000 0.7413 -0.0720 1.0487
  0.4781 0.6268 0.2812 -0.6912 0.1301 0.0510 0.0068 0.6507 0.4527
  0.1350 0.1826 0.3546 0.2278 -0.0508 -0.0651 0.1217 0.1567 0.5288
  0.5086 -0.9875 -0.2722 -0.6188 -0.4074 -0.0436 -0.0204 -0.5911 -0.2062 -
  0.1291 -0.2019 -0.1158 -0.1898 0.0441 -0.0469 0.0920 -0.0552 -0.3413 -
  0.2363 -0.5176 -0.4708 -0.0909 0.0070

- 1.0500 0.9017 0.8258 2.4168 0.6873 0.4999 1.0000 0.5998 0.6002 -
  1.6499 -0.7000 -0.6999 -0.7000 -0.9498 -0.7000 0.7413 -0.0720 1.0487
  0.4781 0.6268 0.2812 -0.6912 0.1301 0.0510 0.0068 0.6507 0.4527
  0.1350 0.1826 0.3546 0.2278 -0.0508 -0.0651 0.1217 0.1567 0.5288
  0.5086 -0.9875 -0.2722 -0.6188 -0.4074 -0.0436 -0.0204 -0.5911 -0.2062 -
  0.1291 -0.2019 -0.1158 -0.1898 0.0441 -0.0469 0.0920 -0.0552 -0.3413 -
  0.2363 -0.5176 -0.4708 -0.0909 0.0070

- 1.0500 0.9214 0.9455 2.3082 0.6382 0.5000 1.0000 0.5999 0.6001 -
  1.8500 -0.7000 -0.7000 -0.7000 -0.6499 -0.7000 0.6752 -0.0920 1.0628
  0.4793 0.5703 0.2508 -0.6334 0.1332 -0.0151 -0.0084 0.8057 0.4788
  0.1207 0.1818 0.2220 0.2147 0.0151 -0.0521 0.1640 0.1596 0.4209
  0.4926 -1.0001 -0.2679 -0.7620 -0.4100 -0.0878 -0.0221 -0.5409 -0.1998 -
  0.1153 -0.2032 -0.1567 -0.1909 0.0897 -0.0432 0.0232 -0.0629 -0.2147 -
  0.2415 -0.4123 -0.4689 -0.0230 0.0104

- 1.0500 0.7214 0.8455 2.3082 0.6382 0.5000 1.0000 0.5999 0.6001 -1.8500 -0.7000 -0.7000 -0.7000 -0.6499 -0.7000 0.6752 -0.0920 1.0628 0.4793 0.5703 0.2508 -0.6334 0.1332 -0.0151 -0.0084 0.8057 0.4788 0.1207 0.1818 0.2220 0.2147 0.0151 -0.0521 0.1640 0.1596 0.4209 0.4926 -1.0001 -0.2679 -0.7620 -0.4100 -0.0878 -0.0221 -0.5409 -0.1998 -0.1153 -0.2032 -0.1567 -0.1909 0.0897 -0.0432 0.0232 -0.0629 -0.2147 -0.2415 -0.4123 -0.4689 -0.0230 0.0104

E.4)Resultado para Caso Teste

```
» regrasdb1
Entre com nome do arquivo de dados: 'caso_tensao_teste.txt'
Entre com número de entradas: 10
Entre com número de colunas: 59
Entrada:     1   +0.994   +0.985   Resultado: NORMAL
Entrada:     2   +0.900   +0.850   Resultado: ANORMAL
Entrada:     3   +0.982   +0.960   Resultado: NORMAL
Entrada:     4   +0.882   +0.910   Resultado: ANORMAL
Entrada:     5   +0.929   +0.916   Resultado: NORMAL
Entrada:     6   +0.829   +0.906   Resultado: ANORMAL
Entrada:     7   +0.922   +0.926   Resultado: NORMAL
Entrada:     8   +0.902   +0.826   Resultado: ANORMAL
Entrada:     9   +0.921   +0.946   Resultado: ANORMAL
Entrada:    10   +0.721   +0.846   Resultado: ANORMAL
```

E.5)Saída do Módulo Estimador de Estados para caso sem valores corrompidos de tensão

```
File: sefv02.dat

SIXBUS POWER FLOW SAMPLE SYSTEM
-------------------------------

Number of Buses = 6
Numbar of Lines = 11
Number of Transformers = 0
Number of Measurements = 34
Number of Voltage Magnitude Measurements = 3
Number of Voltage Angle Measurements = 3
Number of Injection Measurements = 6
Number of Flow Measurements = 22


Branch Data in Per Unit

Branch  From  To    Branch  Branch  Line      Tap   Tap
Type    Bus   Bus     R       X     Charging  Bus   Ratio
------  ----  ----  ------  ------  --------  ----  ------
 LINE      1     2  0.1000  0.2000  0.020000
 LINE      1     4  0.0500  0.2000  0.020000
 LINE      1     5  0.0800  0.3000  0.030000
 LINE      2     3  0.0500  0.2500  0.030000
 LINE      2     4  0.0500  0.1000  0.010000
 LINE      2     5  0.1000  0.3000  0.020000
 LINE      2     6  0.0700  0.2000  0.025000
 LINE      3     5  0.1200  0.2600  0.025000
 LINE      3     6  0.0200  0.1000  0.010000
 LINE      4     5  0.2000  0.4000  0.040000
 LINE      5     6  0.1000  0.3000  0.030000

Bus Voltage Magnitude Measurements in Per Unit

Bus     Voltage    Standard
Number  Magnitude  Deviation
------  ---------  ---------
     1    1.05000    0.00010
     4    0.98184    0.00010
     6    0.96023    0.00010

Bus Voltage Angle Measurements in Per Unit (i.e. Radians)
```

```
Bus      Voltage   Standard
Number   Angle     Deviation
------  ---------  ---------
     1    0.00000    0.00010
     4   -0.07849    0.00010
     6   -0.14844    0.00010

Bus Injection Measurements in Per Unit (100 Mva Base)

Bus     Mw         Standard   Mvar       Standard
Number  Injection  Deviation  Injection  Deviation
------  ---------  ---------  ---------  ---------
     1    1.30064    0.01000    0.29742    0.01000
     2    0.50000    0.01000    1.00000    0.01000
     3    0.60000    0.01000    0.60000    0.01000
     4   -0.55000    0.01000   -0.70000    0.01000
     5   -0.70000    0.01000   -0.70000    0.01000
     6   -1.05000    0.01000   -0.70000    0.01000

Branch Flow Measurements in Per Unit (100 Mva Base)

From  To               Standard              Standard
Bus   Bus    Mw Flow   Deviation  Mvar Flow  Deviation
----  ----  ---------  ---------  ---------  ---------
   1     2    0.39376    0.01000   -0.12771    0.01000
   1     4    0.46833    0.01000    0.23456    0.01000
   1     5    0.43856    0.01000    0.19056    0.01000
   2     1   -0.37868    0.01000    0.11434    0.01000
   2     3    0.09158    0.01000    0.01145    0.01000
   2     4    0.19487    0.01000    0.45430    0.01000
   2     5    0.17284    0.01000    0.18948    0.01000
   2     6    0.41939    0.01000    0.23044    0.01000
   3     2   -0.09111    0.01000   -0.07255    0.01000
   3     5    0.12894    0.01000    0.16035    0.01000
   3     6    0.56216    0.01000    0.51220    0.01000
   4     1   -0.45539    0.01000   -0.22416    0.01000
   4     2   -0.18303    0.01000   -0.45099    0.01000
   4     5    0.08842    0.01000   -0.02485    0.01000
   5     1   -0.42097    0.01000   -0.18527    0.01000
   5     2   -0.16591    0.01000   -0.20855    0.01000
   5     3   -0.12303    0.01000   -0.19660    0.01000
   5     4   -0.08676    0.01000   -0.04716    0.01000
   5     6    0.09667    0.01000   -0.06241    0.01000
   6     2   -0.40361    0.01000   -0.23523    0.01000
   6     3   -0.55087    0.01000   -0.47538    0.01000
   6     5   -0.09552    0.01000    0.01061    0.01000

Building R inverse.

************************************************************

                    ITERATION 1

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  3.4E+06
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is -0.14845 at bus 6
Maximum magnitude mismatch is 0.05005 at bus 1

************************************************************

                    ITERATION 2

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  3.4E+01
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
```

```
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is 0.00126 at bus 3
Maximum magnitude mismatch is 0.00104 at bus 3

************************************************************

                    ITERATION 3

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  1.1E-05
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is -0.00000 at bus 3
Maximum magnitude mismatch is -0.00000 at bus 3
Building delta Z.
Calculating the residual J.
The final value of the residual J is  7.3E-17

State Estimator Solution:

file: sefv02.dat

SIXBUS POWER FLOW SAMPLE SYSTEM
-------------------------------

From Volt.  Volt.   Mw       Mvar    To    Mw      Mvar    Mva
Bus  Mag.   Angle   Injec.   Injec.  Bus   Flow    Flow    Flow
---- ------ ------ -------- -------- ---- ------- ------- -------

   1 1.0500  0.000  130.06   29.74
                                      2   39.38  -12.77   41.39
                                      4   46.83   23.46   52.38
                                      5   43.86   19.06   47.82

   2 1.0361 -4.709   50.00  100.00
                                      1  -37.87   11.43   39.56
                                      3    9.16    1.14    9.23
                                      4   19.49   45.43   49.43
                                      5   17.28   18.95   25.65
                                      6   41.94   23.04   47.85

   3 1.0214 -5.831   60.00   60.00
                                      2   -9.11   -7.26   11.65
                                      5   12.89   16.03   20.58
                                      6   56.22   51.22   76.05

   4 0.9818 -4.497  -55.00  -70.00
                                      1  -45.54  -22.42   50.76
                                      2  -18.30  -45.10   48.67
                                      5    8.84   -2.48    9.18

   5 0.9588 -6.483  -70.00  -70.00
                                      1  -42.10  -18.53   45.99
                                      2  -16.59  -20.86   26.65
                                      3  -12.30  -19.66   23.19
                                      4   -8.68   -4.72    9.88
                                      6    9.67   -6.24   11.51

   6 0.9602 -8.505 -105.00  -70.00
                                      2  -40.36  -23.52   46.72
                                      3  -55.09  -47.54   72.76
                                      5   -9.55    1.06    9.61


Mw losses   =   10.06
Mvar Losses =  -20.26
```

E.6)Saída do Módulo Estimador de Estados para caso com valores corrompidos de tensão

```
File: sefv07.dat
SIXBUS POWER FLOW SAMPLE SYSTEM
------------------------------

Number of Buses = 6
Numbar of Lines = 11

Number of Transformers = 0
Number of Measurements = 34
Number of Voltage Magnitude Measurements = 3
Number of Voltage Angle Measurements = 3
Number of Injection Measurements = 6
Number of Flow Measurements = 22


Branch Data in Per Unit

Branch  From  To    Branch  Branch  Line      Tap   Tap
Type    Bus   Bus     R       X     Charging  Bus   Ratio
------  ----  ----  ------  ------  --------  ----  ------
 LINE      1     2  0.1000  0.2000  0.020000
 LINE      1     4  0.0500  0.2000  0.020000
 LINE      1     5  0.0800  0.3000  0.030000
 LINE      2     3  0.0500  0.2500  0.030000
 LINE      2     4  0.0500  0.1000  0.010000
 LINE      2     5  0.1000  0.3000  0.020000
 LINE      2     6  0.0700  0.2000  0.025000
 LINE      3     5  0.1200  0.2600  0.025000
 LINE      3     6  0.0200  0.1000  0.010000
 LINE      4     5  0.2000  0.4000  0.040000
 LINE      5     6  0.1000  0.3000  0.030000

Bus Voltage Magnitude Measurements in Per Unit

Bus     Voltage    Standard
Number  Magnitude  Deviation
------  ---------  ---------
     1    1.05000    0.00010
     4    0.88184    0.00010
     6    0.91023    0.00010

Bus Voltage Angle Measurements in Per Unit (i.e. Radians)

Bus      Voltage   Standard
Number   Angle     Deviation
------  ---------  ---------
     1    0.00000    0.00010
     4   -0.07849    0.00010
     6   -0.14844    0.00010

Bus Injection Measurements in Per Unit (100 Mva Base)

Bus     Mw         Standard   Mvar       Standard
Number  Injection  Deviation  Injection  Deviation
------  ---------  ---------  ---------  ---------
     1    1.30064    0.01000    0.29742    0.01000
     2    0.50000    0.01000    1.00000    0.01000
     3    0.60000    0.01000    0.60000    0.01000
     4   -0.55000    0.01000   -0.70000    0.01000
     5   -0.70000    0.01000   -0.70000    0.01000
     6   -1.05000    0.01000   -0.70000    0.01000

Branch Flow Measurements in Per Unit (100 Mva Base)

From  To               Standard              Standard
Bus   Bus    Mw Flow   Deviation  Mvar Flow  Deviation
----  ----  ---------  ---------  ---------  ---------
   1     2    0.39376    0.01000   -0.12771    0.01000
   1     4    0.46833    0.01000    0.23456    0.01000
   1     5    0.43856    0.01000    0.19056    0.01000
   2     1   -0.37868    0.01000    0.11434    0.01000
   2     3    0.09158    0.01000    0.01145    0.01000
   2     4    0.19487    0.01000    0.45430    0.01000
```

```
   2     5    0.17284    0.01000    0.18948    0.01000
   2     6    0.41939    0.01000    0.23044    0.01000
   3     2   -0.09111    0.01000   -0.07255    0.01000
   3     5    0.12894    0.01000    0.16035    0.01000
   3     6    0.56216    0.01000    0.51220    0.01000
   4     1   -0.45539    0.01000   -0.22416    0.01000
   4     2   -0.18303    0.01000   -0.45099    0.01000
   4     5    0.08842    0.01000   -0.02485    0.01000
   5     1   -0.42097    0.01000   -0.18527    0.01000
   5     2   -0.16591    0.01000   -0.20855    0.01000
   5     3   -0.12303    0.01000   -0.19660    0.01000
   5     4   -0.08676    0.01000   -0.04716    0.01000
   5     6    0.09667    0.01000   -0.06241    0.01000
   6     2   -0.40361    0.01000   -0.23523    0.01000
   6     3   -0.55087    0.01000   -0.47538    0.01000
   6     5   -0.09552    0.01000    0.01061    0.01000

Building R inverse.

************************************************************

                    ITERATION 1

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  5.4E+06
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is -0.14844 at bus 6
Maximum magnitude mismatch is -0.11558 at bus 4

************************************************************

                    ITERATION 2

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  2.3E+04
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is 0.00540 at bus 3
Maximum magnitude mismatch is 0.00606 at bus 2

************************************************************

                    ITERATION 3

Building H matrix.
Building H transpose R inverse H.
Building delta Z.
Calculating the residual J.
The residual J is  2.2E+04
Building H transpose R inverse delta Z.
Calculating and storing the table of factors.
Using the table of factors to calculate delta V.
Updating the bus voltages.
Maximum angle mismatch is -0.00005 at bus 3
Maximum magnitude mismatch is -0.00003 at bus 5
Building delta Z.
Calculating the residual J.
The final value of the residual J is  2.2E+04

State Estimator Solution:

file: sefv07.dat

SIXBUS POWER FLOW SAMPLE SYSTEM
-------------------------------
```

From Bus	Volt. Mag.	Volt. Angle	Mw Injec.	Mvar Injec.	To Bus	Mw Flow	Mvar Flow	Mva Flow
1	1.0476	0.006	149.08	116.54				
					2	48.54	12.14	50.04
					4	54.74	71.27	89.87
					5	45.80	33.12	56.52
2	0.9771	-4.630	47.15	90.52				
					1	-46.21	-11.58	47.64
					3	6.35	-2.65	6.88
					4	34.83	72.65	80.57
					5	14.86	13.78	20.26
					6	37.33	18.32	41.58
3	0.9735	-5.580	62.19	61.71				
					2	-6.33	-2.95	6.98
					5	12.90	13.89	18.96
					6	55.62	50.77	75.31
4	0.8840	-4.499	-79.31	-138.35				
					1	-50.92	-59.74	78.49
					2	-31.36	-67.44	74.37
					5	2.97	-11.18	11.56
5	0.9142	-6.483	-63.55	-61.70				
					1	-43.30	-29.57	52.43
					2	-14.37	-15.89	21.42
					3	-12.35	-17.17	21.15
					4	-2.78	5.08	5.79
					6	9.26	-4.16	10.15
6	0.9101	-8.509	-99.54	-65.94				
					2	-35.99	-18.96	40.68
					3	-54.40	-46.46	71.54
					5	-9.15	-0.52	9.17

Mw losses = 16.03
Mvar Losses = 2.78