UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA QUÍMICA
DEPARTAMENTO DE ENGENHARIA DE SISTEMAS QUÍMICOS

AREA DE CONCENTRAÇÃO:

SISTEMAS DE PROCESSOS QUÍMICOS E INFORMÁTICA

LABORATÓRIO DE CONTROLE E AUTOMAÇÃO DE PROCESSOS (LCAP)

RICARDO AUGUSTO DE ALMEIDA

Desenvolvimento de um Sistema de Controle Remoto para Acionamento e monitoramento de Processos Químicos - CRAPQ

Dissertação de mestrado apresentada ao Curso de Pós-Graduação da Faculdade de Engenharia Química, da Universidade Estadual de Campinas, como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Química.

Orientador: Prof. Dr. Flávio Vasconcelos da Silva

Campinas/SP/BRASIL

Abril – 2010

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Almeida, Ricardo Augusto
AL64d Desenvolvimento de um sistema de Controle Remoto para Acionamento e monitoramento de Processos Químicos - CRAPQ / Ricardo Augusto de Almeida. -- Campinas, SP: [s.n.], 2010.

Orientador: Flávio Vasconcelos da Silva.
Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Química.

1. Controle remoto. 2. Monitoramento. 3. Controle automático. 4. Sensoriamento remoto. 5. Automação industrial. I. Silva, Flávio Vasconcelos da. II. Universidade Estadual de Campinas. Faculdade de Engenharia Química. III. Título.

Título em Inglês: Development of a Remote Control system for operating and monitoring of Chemical Processes - CRAPQ
Palavras-chave em Inglês: Remote control, Monitoring, Automatic control, Remote sensing, Industrial automation
Área de concentração: Sistemas de Processos Químicos e Informática
Titulação: Mestre em Engenharia Química
Banca examinadora: Ana Maria Frattini Fileti, Flávio Matsuyama
Data da defesa: 16/04/2010
Programa de Pós Graduação: Engenharia Química

Dissertação de Mestrado defendido por Ricardo Augusto de Almeida e aprovada em 16 Abril de 2010 pela banca examinadora constituída pelos doutores:

Prof. Dr. Flávio Vasconcelos da Silva
(UNICAMP/FEQ/DESQ)
ORIENTADOR

Prof. Dra. Ana Maria Frattini Fileti
(UNICAMP/FEQ/DESQ)

Prof. Dr. Flávio Matsuyama
(UNIABC)

Este exemplar corresponde à versão final da Dissertação de Mestrado em Engenharia Química defendida por Ricardo Augusto de Almeida em 16 Abril de 2010.

Prof. Dr. Flávio Vasconcelos da Silva

Dedico este trabalho a minha esposa Flávia Pereira Nascimento de Almeida, o meu pai José Sebastião de Almeida, a minha mãe Rosa Maria de Almeida, a minha irmã Maria Luiza de Almeida e meus filhos Fabio Augusto Nascimento de Almeida e Beatriz Ludmila Nascimento de Almeida.

"Vinde a mim, todos os que estais cansados e sobrecarregados, e eu vos aliviarei. Tomai sobre vós o meu jugo e aprendei de mim, porque sou manso e humilde de coração; e achareis descanso para a vossa alma. Porque o meu jugo é suave, e meu fardo é leve." *Yeshua Nâẓərat*

AGRADECIMENTOS

À Deus por prover de saúde, esperança, e amor nada seria realizado sem a força de Seu amor.

Ao Nosso Mestre maior Jesus de Nazaré com muito amor.

Aos Mentores e Amigos espirituais que me guiam, sem suas inspirações e auxílio não conseguiria agregar nenhuma sábia decisão nesta passagem.

À minha esposa e companheira Flávia que em momentos de vacilo socorreu-me com extrema dedicação.

Ao papai José e a mamãe Rosa que conseguiram vencer barreiras intransponíveis para muitas pessoas, fazendo seu filho vencer mais esta etapa de cabeça erguida e honesta.

À minha amada irmã Luiza e seu esposo Luis Mauro, devo tanto que um livro de agradecimentos seria pouco.

Aos meus filhos Fábio Augusto e Beatriz Ludmila, pois são eles as inspirações de querer sempre fazer o melhor.

Aos vovós Ovídio e Maria (em memória) a saudade é imensa.

Ao professor Flávio Vasconcelos pela orientação, paciência, dedicação, mas principalmente por ter a oportunidade de ser amigo de um homem de bem.

À professora Ana Maria Frattini pela confiança, paciência, apoio e pela amizade, essenciais durante todo o trabalho.

Ao professor Flávio Matsuyama pela orientação e por dar fé em todo trabalho desde a graduação até os dias de hoje, sua colaboração e amizade foram determinantes para a conclusão de mais este trabalho.

Ao professor José Vicente Halak D' Ângelo pela paciência e oportunidade de aprender e trabalhar juntos.

À Sr. Oscar (em memória), D. Cleusa, Lucy, Fabiana, Lucas apoiando sempre, uma família abençoada.

Aos parentes e amigos, Reinaldo e Ivone, Rosangela e James, Leilane e Werverly, Alessandro e Rita, Eduardo e Valentina, Lilian e Álvaro, Heraldo e Vera, Josiane e Clovis, Célia e Emerson, Marcos e Jemima, Sandra e Luís, Gilmar, Odair e Silvia, Gislaine, Sonia, Iara, Paulo e Áurea, Marcos e Elza, Isabel, Antonia, Jesus Lucas e Verenice, Leonildo e Rosa, Osmir e Aparecida, Antonio e Terezinha, Antonio e Inês, Carlos e Rita, José e Rosa, Roberto, Inesinha, João Leite e Vilma, Douglas, Patrícia, José Ribeiro e Antonia, pelos momentos alívio e lazer durante a exaustão do dia-a-dia.

Aos amigos do LCAP, Wagner, Thiago Pinelli, Regina, por serem o alicerce no início desta jornada.

Aos companheiros e amigos do LCAP Manuela, Tatiane, Camila, Marcelle, Renata, Ivan, Marcelo, Thiago Costa, Georges, Rodrigo, Fernando, Luiz, Rejane, Miguel, Alexandre, Athaualpa, Lilian, Paula, pela força de cada dia no laboratório.

Aos amigos Kleber e Janaina, Evangelista pela amizade, alegria e esperança que sempre apoiaram nas horas difíceis.

À amiga Cristiane Zanuto pela amizade, fé e perseverança, em fazer sempre o melhor e o correto mesmo momentos que ficamos sem chão.

À amiga Marisa David pela alegria e afeto dedicados por sua pura empatia, numa amizade verdadeira cuja admiração é inestimável.

Aos amigos da República Gringos, Alexandre, André, Ricardo Malveira, Túlio, Pedro Ivo, Péricles, Cesar, Vinícius, José, Lorival, Rafael, Lucas, Pedro Henrique, José Luiz, Lineu, Daniel, Jonathan, Igor, Alisson, Vitor, Guilherme, Ricardo Shiota, Plínio, pelo acolhimento nesta casa maravilhosa.

Aos amigos da Faculdade de Engenharia Química Juliana, Dalva, Mara, Rafael, Charles, Alessandro, Marcelo, Jardel, Rafael, Obsolon, Michele, Melissa, pela amizade e colaboração.

Aos Professores Roger, Franciscone, Cobo, Bete, Elias, Sandra, Kakuta, Maria Tereza, pela confiança e respeito que passaram durante todo o curso.

Aos amigos do Jornal O Estado de S. Paulo Vitor, Giora, Reinaldo, Douglas, Adilson, Samuel, Rafael, Flávio, Daniel, João Carlos, João Romero, Nagata, Pedro, Marcos, Luis, Edson, Dias, Franco, Lucio, Odair pela amizade e experiência de profissional.

Aos técnicos da Faculdade de Engenharia Química Juliano, Waldemir, Marcos e Rafael pela amizade, boa vontade e apoio.

Às secretárias Márcia, Valquíria, Lúcia e Maria Elvira pela colaboração e atenção.

Aos funcionários da Faculdade de Engenharia Química – UNICAMP pela colaboração.

À UNICAMP pelo acolhimento e estrutura.

Ao CNPq e a CAPES pelo apoio financeiro.

A capela de Nossa Senhora Imaculada Conceição, e a paróquia de Nossa Senhora Aparecida e Nossa Senhora do Carmo em Santo André pela fé que moldou o meu coração.

As Casas Espíritas Lar de Maria, Simão e Pedro, Casa de Jesus que me abriram um novo horizonte entre Ciência e a Religião.

RESUMO

Os equipamentos e aparelhos contemporâneos utilizados em diversas aplicações do cotidiano doméstico e industrial agregam tecnologia suficiente para serem acionados a distância por diversos meios físicos de comunicação. Estes meios físicos evoluíram de um simples aparelho televisor acionado via luz infra-vermelha, até um braço robótico controlado pela Estação Internacional Espacial via sinais digitais por micro-ondas (KAUDERER, 2007).

Seguindo esta tendência, as indústrias químicas, petroquímicas e bioquímicas têm instalado diversos equipamentos e instrumentos que podem ser controlados remotamente (SMAR, 2004). Atualmente é de suma importância que o monitoramento e controle de plantas químicas e processos de manufatura possam ser realizados a distância. Portanto o controle e o monitoramento remoto são imprescindíveis em locais de risco a saúde do homem, ou mesmo em locais de difícil acesso a dispositivos e instrumentos.

Com a predominância dos computadores pessoais (PC) em aplicações industriais pode-se atribuir maior abrangência ao controle de processos computadorizados, facilitando a implementação de sistemas de acionamento remoto via redes de comunicações digitais.

Este trabalho teve como principal objetivo, desenvolver um projeto capaz de administrar e acionar a distância algoritmos científicos e industriais através de Redes Virtuais Privadas (*VPN*). Os programas acessados pelas *VPN's* desenvolvem ambientes para Supervisão e Interface Homem Máquina (IHM), na área de pesquisa para controle de processos químicos e biotecnológicos.

No ambiente de desenvolvimento tipo Controle de Supervisório e Aquisição de Dados (*SCADA*), foram desenvolvidas as aplicações para a supervisão de três processos químicos, um reator de precipitação da bromelina do abacaxi, um reator de biodiesel e um sistema de refrigeração, no Laboratório de Controle e Automação de Processos (LCAP/FEQ/UNICAMP).

O desenvolvimento de um sistema remoto composto de três Servidores de VPN's, um Servidor de Internet Seguro resultaram num Ambiente Virtual de interação remota que propiciou interoperabilidade dos três experimentos no LCAP, de modo que novos experimentos possam ser agregados futuramente ao sistema com segurança e simplicidade.

Palavras-chaves:Controle remoto,Monitoramento,Automação Industrial,Sensoriamento remoto.

ABSTRACT

Apparatus used in many contemporary applications of everyday in household and industry, got enough technology to be implement remote control actions and remote monitoring by diverse physical means of communications. Those physical means of communications were evoluting, starting of a simple TV apparatus controlled by infrared LED until a robot arm controlled by International Space Station by exchange digital communication microwave signal way (KAUDERER, 2007). The Chemical Industry, Oil Refinery Industry and Biochemical Industry are following this tendency because the remote monitoring and control remote of chemical plants are very principal where there danger the human heath's or local of difficult access by devices and instruments. In this context, currently industries made installing of many remote devices controlled (SMAR, 2004).

With the major difusion of personal computers (PC) at industry applications there were a bigger abrangency at controll of process computed, who collaborating to easily implement the actioning by means remote networks of digital communications.

The goal of this work was developing a project whose enabled management and the actioning of scientific computing algoritms and of algoritms of industry applications, by the means Virtual Private Networks (VPN). The access by VPN in development programs of Human Interface Machine (HIM) and Supervisory was made in area of control process chemical and biochemical.

In this ambient of building the supervisory control and data acquisition (SCADA) the remote monitoring and the remote supervisory was use to of three apparatus, who are: a biodiesel reactor, a refrigeration system and a bromelin precipitation reactor. Those three apparatus were installed at Laboratory Control Automation of Chemicals Process (LCAP/FEQ/UNICAMP).

The project was compost by three Servers of VPN and one Server secure of Internet, maintaining interoperability between apparatus with same or similar interactivity at of local user in SCADA systems installed's LCAP. In the future more apparatus can to be installed in project with security and simplicity.

Keywords: Remote Control, Monitoring, Industrial Automation, Remote sensing.

SUMÁRIO

INDICE DE FIGURAS

INDICE DE TABELAS

1. INTRODUÇÃO.

Existem no mercado industrial uma vasta variedade de interfaces homem máquina, controladores lógicos programáveis (CLP), sistemas operacionais (S.O.) e sistemas SCADA que necessitam de uma maior integração e interoperabilidade.

Os meios de controle e aquisição de dados são indispensáveis na indústria atual e diversas tecnologias são desenvolvidas para área de automação. Neste contexto tecnológico surgiram as redes de comunicação digitais com protocolos de comunicação que trabalham com maior desempenho em aplicações industriais.

Hoje com a difusão da rede mundial de computadores ("*World Wide Web"*), faz-se necessário que os dados e informações trafeguem via protocolo de controle e transporte e protocolo de internet ("*TCP/IP"*) por distâncias extracontinentais. Os dados ou informações que são disponibilizados por redes industriais ou na internet para aplicações da indústria devem ser computados por equipamentos independente da IHM, sistema SCADA, CLP ou se restrinjam a S.O. e a protocolos dedicados.

A compatibilidade entre multiplataformas (interoperabilidade) na supervisão e controle de processos químicos a distância é o foco deste trabalho. Assim será explanado o desenvolvimento do Sistema de Controle Remoto para Automação de Processos Químicos (SCRAPQ - I), por meio de três redes virtuais privadas ("*VPN"*).

Neste trabalho foi desenvolvido um ambiente virtual de interação que propiciou a integração de aplicações SCADA, utilizando tecnologias de segurança e criptografia muito utilizadas na internet, tais como; verificação do ponto de internet ("*IP"*), *"Secure Shell"* ("*SSH"*) e tunelamento de informação (KOMPELLA e REKHTER, 2006). Trabalhando com estes três mecanismos de segurança na internet, foi viabilizado o acionamento e supervisão de dados dos diversos sistemas de automação do laboratório, indiferente do supervisório, CLP, protocolo de controle ou plataforma operacional, assim a arquitetura do sistema desenvolvido no CRAPQ demonstrou ser uma forte ferramenta na indústria e no meio acadêmico.

A arquitetura do CRAPQ foi desenvolvida para ser um sistema apto a trazer um realismo de operação local a profissionais e alunos, e capaz de acessar ambientes de plantas industriais e experimentos com similar interação do usuário local, mostrando, em tempo real, todos os eventos e alarmes do processo.

1.1 OBJETIVOS.

O objetivo geral deste trabalho foi desenvolver um sistema que realiza-se a administração remota, monitoramento remoto e o acionamento remoto de diversas arquiteturas de sistemas, em ptotótipos industriais distintos, que interagissem nos diferentes S.O do cliente externo. O projeto utilizou programas que são livre de licença do fabricante ("*Freewares"*) e programas de código aberto ("*Open Source"*), compatíveis com a plataforma JAVA® , C®. Considerando o objetivo geral foram definidos os seguintes objetivos específicos:

- Acessar e acionar a rede industrial "*Fieldbus Foundation®"* (FF-H1) que controla os reatores adaptáveis ao produto (Multipropósito), através da rede *Ethernet* de alta velocidade (FF-HSE). Conectando a esta rede via comutador de rede local (*Ethernet* padrão IEEE 802.3).
- Acessar e acionar o CLP do fabricante Hi® que controla a planta de refrigeração. Conectando a uma rede sem fio via comutador de rede sem fio (padrão IEEE 802.11).
- Estabelecer uma transferência segura de dados entre cliente da internet e servidor SCADA, cujo acesso a internet é feito através do servidor de internet.
- Criar as redes virtuais privadas entre os servidores SCADA e o servidor de internet.
- Acionar variáveis de entrada e saída, CLP ou dispositivo de interface fieldbus ("*DFI"*).
- Realizar reconhecimento de alarme no CLP ou DFI.
- Gerenciar os sistemas e subsistemas remotamente (SCADA ou processos de máquina).

- Ligar e desligar o sistema remotamente.
- Administrar os servidores SCADA através do cliente de internet nas redes virtuais privadas em funcionamento na rede local, respeitando as taxas de transmissão dos equipamentos locais.

1.2 JUSTIFICATIVAS.

Houve uma abrupta evolução tecnológica na automação industrial e na ciência da computação. Surgiram dispositivos, equipamentos e aplicativos que facilitam a configuração, instalação e administração de CLP, sistemas digital de controle distribuído (SDCD), sistemas integrados de gestão empresarial ("*ERP*") e sistemas SCADA. Tais tecnologias integram e gerenciam processos complexos da indústria em multiplataformas, gerando relatórios e servindo como base a gestão financeira online de empreendimentos.

Com a pluralidade tecnológica e a diversidade de fabricantes usando tecnologias dedicadas, a problemática da portabilidade de aplicações em sistemas tem sido atenuante fator de pesquisa.

Neste projeto a solução para a integração e controle de diferentes arquiteturas de sistemas foi possível, graças a associação de aplicações desenvolvidas em Plataforma C® e JAVA®**.** As aplicações TigthVNC® e Logmein® de utilização livre de licença (*"Freeware"*) acessam sistemas remotamente criando três VPN's híbridas, sendo uma alternativa simples, eficaz, robusta e segura. A utilização de tais aplicações para VPN's, compatíveis com plataforma JAVA® facilita a interoperabilidade, pois a compilação de tais programas não estão atrelados às arquiteturas dos S.O.'s.

Atualmente os S.O's modernos possuem programas que estabelecem a interface entre o núcleo de processamento físico (**"***Kernel***"**) e um núcleo de processamento de outro S.O, esta interface criada pela SUN Microsystem® é chamada de máquina virtual JAVA® ("*JVM"*).

A JVM realiza a compilação dos programas por meio de códigos binários virtuais (*"bytecodes"*), provendo que aplicações sejam executadas remotamente em máquinas que disponibilizam serviços (servidores), sem que estejam instaladas na máquina que acessam estes serviços (clientes).

A associação destas tecnologias para o uso na segurança da comuniacação de dados entre servidores e clientes, e na administração remota colaboram para viabilizar o controle e automação de sistemas industriais à distância, conforme estudo do autor Creey e Byres realizado em 2005. Assim devido à robustez de configuração oferecida pelos programas de VPN's desenvolvidos nestas tecnologias, e o custo benefício atender a quaisquer sistema de automação e controle de processo computadorizado atual, tornou-se viável desenvolver um projeto que pode ser utilizado em diferentes interfaces de clientes remotos. As interfaces do usuário dos S.O's atuais testadas, são de desenvolvedores conhecidos no mercado de informáica mundial atual (Sun Microsystems®,Microsoft®, Debian®) podendo ser atualizadas continuamente mantendo toda interoperabilidade do projeto CRAPQ.

2. FUNDAMENTAÇÃO TEÓRICA E REVISÃO BIBLIOGRÁFICA.

2.1. Histórico da Automação Industrial.

As décadas de 60 e 70 marcam a fase de surgimento dos CLP's na automação industrial o que mudou completamente o cenário das indústrias no mundo.

Originalmente os CLP's foram usados em aplicações de controle discreto (Liga/Desliga), como os sistemas a relés, eram facilmente instalados, economizando espaço e energia, além de possuírem indicadores de diagnósticos que facilitavam a manutenção.

Qualquer necessidade de alteração na lógica de controle da máquina era realizada em pouco tempo, sendo necessárias apenas mudanças em linhas do programa, sem necessidade de alterações físicas nas ligações elétricas.

Com as inovações tecnológicas dos microprocessadores (Motorola®, Mitsubish®, Intel®, Atlon®) houve maior flexibilidade na construção e desenvolvimento de novos equipamentos. Acrescentando funções inteligentes aos CLP's os microprocessadores incorporaram os seguintes avanços:

- 1972 – Funções de temporização e contagem;
- 1973 - Operações aritméticas, manipulação de dados e comunicação com computadores;
- 1974 – Comunicação com Interfaces Homem Máquina;
- 1975 – Maior capacidade de memória, controles analógicos e funções de controle de processos;
- 1979/80 – Módulos de E/S (Entradas e Saídas) remotos, módulos inteligentes e controle de posicionamento.

Nos anos 80, aperfeiçoamentos foram atingidos fazendo do CLP um dos equipamentos mais atraentes na Automação Industrial.

A possibilidade de comunicação em rede (1981) é hoje uma característica indispensável na indústria.

Além da comunicação em rede e das diversas funções, foi atingido um alto grau de otimização tanto no número de pontos monitorados como no tamanho físico. Esta otimização do CLP possibilitou o surgimento de minis e micros CLP's a partir de 1982 (Modicon®) e tornou o equipamento mais popular, principalmente em pequenas aplicações industriais.

Atualmente, os CLP's apresentam as seguintes características:

- Módulos de entradas e saída (E/S) com grande número de pontos por módulo (Módulos de Alta Densidade);
- Módulos de E/S remotos controlados por uma mesma unidade de processamento de dados (UCP);
- Módulos com co-processadores que permitem realização de funções de controle proporcional integral e derivativo (PID);
- Modulos especifícos para o posicionamento de eixos e sincronismo de motores;
- Modulos de transmissão em rede para diversos protocolos fieldbus;
- Modulos de leitura de códigos de barras;
- Aplicativos de programação em S.O Microsoft® (mais utilizados em PC após 1995);

- Integração de CLP's entre banco de dados, aplicativos de planilhas eletrônicas, aplicativos editores texto, ambientes de desenvolvimento de programas (Access®, Excel®, Visual Basic®) via bibliotecas de associações dinâmicas (*dll*);
- Recursos de monitoramento da execução do programa, diagnósticos e detecção de falhas;
- Instruções avançadas que permitem operações entre dispositivos através de proces-sadores dedicados como os sistemas da Echelon®;
- Processamento paralelo (com opção de redundância), proporcionando confiabilidade na utilização de processadores dedicados;
- Pequenos e micros CLP's que oferecem recursos de dispositivos e aplicações nos CLP's de grande porte como os da Siemens®, RockWell®, ABB® e Schneider®;
- Conexão de CLP's em redes industriais de diversos protocolos e redes locais.
- Acesso a E/S pela internet através de servidor de pagina de internet incorporado.
- Aplicações de monitoramento e supervisão (Elipse E3®, Indusoft®).
- Adaptação de redes industriais para controle de processos em aplicações da indústria química, petroquímica e biotecnológica.

Fonte de informação dos fabricantes: Schneider®, Siemens®, RockWell®, SMAR®.

2.2. Automação de Sistemas Químicos.

O controle de processos químicos é realizado tradicionalmente por meio de CLP's, SDCD's, IHM's, controladores de interface periférica (*PIC*) com funções PID e Sistemas SCADA (NATALE, 2004).

Atualmente houve um crescimento considerável na utilização de sistemas distribuídos (SD)**,** para o controle e monitoramento na indústria química, petroquímica e de manufatura (SMAR®, 2002). Principalmente devido aos novos padrões de comunicação entre computadores e equipamentos de automação industriais (OPC®, 2007).

Os dispositivos de medição e atuação no campo chamados de dispositivos inteligentes de campo (DI's) são frequentemente utilizados em novas aplicações ou em re-engenharia de equipamentos em funcionamento.

Segundo estudo realizado por Santos (2006), conclui-se que anteriormente a automação industrial visava especificamente a manutenção da qualidade do produto final, através da redução da variabilidade dos parâmetros dos processos. Atualmente a utilização de técnicas de instrumentação e controle em sistemas biotecnológicos, vem agregando confiabilidade, e reduzindo os custos energéticos, assim o aperfeiçoamento da supervisão melhora da qualidade dos produtos finais. Portanto a supervisão em tempo real destes sistemas biotecnológicos é considerada tão importante, pois assim colaboram para o aumento da produtividade e a redução dos devios no ponto de ajuste (*"set-point"*- SP) do processo.

Exemplos de aplicação de sistemas distribuídos com dispositivos inteligentes são utilizados nos caso-estudo I e II de:

- Produção do biodiesel em batelada (SANTOS, 2006);
- Precipitação bromelina do abacaxi (LEITE e FUJIKI, 2008).

Os DI estão instalados em reatores adaptáveis ao processo (Multipropósito) no Laboratório de Controle e Automação de Processos na Faculdade de Engenharia Química da Unicamp (LCAP – FEQ).

Os SD / DI controlam processos químicos e detém as seguintes características:

- Interoperabilidade;
- Agilidade na instalação e configuração;
- Redução de custos de instalação;
- Agilidade na manutenção corretiva;
- Facilidade na execução de planos para manutenção preventiva e preditiva;
- Redução dos custos de manutenção;
- Reconciliação de dados.

Além de oferecer um maior desempenho no processamento de informações do processo, possibilitando implementar estratégias de controle sofisticadas de forma simples através de aplicativos de cálculos científicos (Matlab® e Scilab®) e Blocos de Funções para desenvolvimento de lógicas e estratégias matemáticas.

Os blocos de funções como os de E/S analógicas, E/S digitais, Controladores PD, PI, PID, razão, bias, e ganho foram criados com o objetivo de proporcionar ao sistema de controle distribuído a possibilidade de se dedicar às funções de mais alto nível, como otimização, que foram utilizados por SILVA et al. 2003.

2.3. Utilização de Sistemas Distribuídos.

Os sistemas distribuídos (SD) são sistemas que possuem características de processamento descentralizado, onde os algoritmos são programados de forma modular em unidades de processamento individuais; suas associações (*links*) são feitas através de um canal de comunicação interno ou externo (SMAR®, 2002).

Após o desenvolvimento da metodologia de programação orientada a objeto (POO) com a linguagem de programação SIMULA 67, os SD's passaram a ter uma interface de programação intuitiva.

Atualmente existem dispositivos que executam algoritmos locais e enviam parte de seus dados para outros dispositivos processarem, esta troca de dados e a descentralização de processamento melhora o desempenho e a performance principalmente em algoritmos complexos (CORMEN et al, 2002).

Com a disseminação dos SD's e POO surgiram diversas plataformas de programação, tais como: Dot NET® , JAVA®, VBScript® , PHP® .

Na automação industrial existem diversos equipamentos que funcionam com sistemas distribuídos e programação orientada a objeto, como por exemplo:

- **Foundation Fieldbus® (FF)**:

  Padrão de rede industrial, equipamentos e dispositivos Fieldbus Foundation ® (DI mercado europeu).

- **Actuador Sensor-interface® (AS-i)**:

  Padrão de rede industrial, equipamentos e dispositivos AS-i® (DI mercado alemão).

- **InterBus®**:

  Padrão de rede industrial, equipamentos e dispositivos InterBus Foundation® (DI mercado europeu).

- **DeviceNet®**:

  Padrão de rede industrial, equipamentos e dispositivos Allen Bradley® (DI mercado americano).

- **ProfiBus ®**:

  Padrão de rede industrial Modicon ® (DI mercado alemão).

- **LonWorks ®**:

  Padrão de rede industrial Echelon® divisão RockWell Systems® (DI mercado americano).

Estes são alguns padrões de rede e dispositivos SD/DI aplicados para Automação com características próprias para aplicações de diversos segmentos industriais (ZIELINSK, 2005).

A indústria química e petroquímica e atualmente a indústria de biotecnologia utilizam frequentemente os dispositivos FF**,** devido o padrão antigo **"***Highway Addressable Remote Transducer***"** (HART)**,** sucessor dos dispositivos de transmissão de corrente (padrão 4-20 mA).

2.4. Hierarquia de Sistemas SIGE, SDCD, PLC e SCADA.

As grandes corporações planejam toda sua infra-estrutura de Tecnologia da Informação **(**TI**)** e prevêem um sistema gestor de negócios que pode trocar informações entre filiais e matriz. O sistema que administra a informação que trafega entre diversos servidores de uma companhia é chamado de sistemas integrados de gestão empresarial ou SIGE (*ERP*).

O SIGE é implementado para gerenciar todo trafego de informação que tramita dentro ou entre as filiais e a matriz de negócio (exemplo: SAP®).

Sistema digital de controle distribuído (SDCD) e o Controlador lógico programável (CLP), são sistemas de automação industriais que controlam e monitoram as operações de campo no chão de fabrica.

O SDCD foi particularmente difundido nas indústrias químicas e petroquímicas, devido ao sofisticado nível de diagnóstico oferecido pelo sistema, além da opção à redundância de operações e a característica de transferência e armazenamento de dados.

O custo de manutenção do SDCD era muito elevado e com a sofisticação dos computadores pessoais (*PC*) e CLP's, a indústria de automação tornou estes últimos equipamentos economicamente mais atraentes para o desenvolvimento de aplicações nas áreas industriais de processos. Assim o SDCD passou a desaparecer aos poucos de aplicações de médio e pequeno porte e em alguns casos até em aplicações de grande porte.

A versatilidade dos PC / CLP atuais aliado aos novos sistemas de supervisão de processos industriais SCADA e toda esta hierarquia de sistemas SIGE, são previstas na implementação de uma gestão em *Real-Time* do negócio. (NATALE, 2000), cuja integração entre sistemas de diversos fabricantes é um desafio para engenheiros e desenvolvedores e arquitetos de sistemas.

2.5. Redes Virtuais Privadas (VPN).

As redes de computadores foram desenvolvidas para distribuir serviços e recursos entre diversos usuários a fim de reduzir custos de equipamentos. Numa área onde funciona uma rede local (*LAN*) pode haver muitos computadores interligados fisicamente seja por cabos através de placas de rede ou por sinais de radio frequencia por meio de placas de rede sem fio.

Uma rede virtual privada (*VPN*) emula uma conexão física entre dois computadores de modo que outros computadores não possam decodificar o trafego de dados entre estes computadores. Por isso leva o nome de rede virtual privada, pois mesmo

que estes computadores estejam conectados fisicamente em provedores diferentes que dão acesso a rede mundial de computadores (*WAN*), a VPN conecta os dois computadores tunelando a informação como se estivessem ligados lado a lado por um cabo assim, dividindo recursos somente entre estes (KOMPELLA, 2006).

A VPN utiliza o método de acesso a recurso cliente / servidor e o funcionamento de uma VPN são divididas em seis etapas:

1- Solicitação de acesso do Cliente:

O programa instalado no computador cliente envia a solicitação através de um usuário e senha previamente cadastrado no servidor.

2 - Identificação de usuário pelo Servidor:

O programa instalado no computador servidor recebe a solicitação identifica o usuário cadastrado.

3 - Troca de chaves simétricas entre Cliente e Servidor:

Após a identificação o servidor gera um código de 128 bits ou acima deste valor e o envia para o cliente (chave simétrica).

5 - Criptografia de dados:

Assim que a chave for instalada em cada um dos equipamentos todos os dados a serem transferidos são criptografados por algoritmos como SSH, DES, AES ou IDEA (CORMEN et al, 2002).

6 - Utilização de Comandos:

Os dados enviados por aplicações de VPN são comandos de terminais como TelNet , X-Terminal e protocolos X-Server (TANEMBAUM, 2002).

Alguns exemplos de programas que utilizam este algoritmo são Tigth VNC®, NX-Server®, OpenVPN® (OTANEZ et al, 2002).

Outro método de estabelecer uma VPN é utilizando um servidor de roteamento (*Proxy*). O proxy fornece uma chave pública para que dois computadores de maneira que troquem chaves privadas e estabeleçam as etapas citadas anteriormente. A vantagem deste tipo de configuração é que o proxy fornece o acesso por meio de protocolo de hipertexto (*HTML*) e assim a manipulação de hipertextos criptografados é interpretada por navegadores de internet que viabiliza o uso de qualquer equipamento atual que navegue na rede mundial de computadores.

Um exemplo deste tipo de serviço é o sistema Logmein®, cujo sistema cria um ambiente virtual desenvolvido a partir de hipertextos. As duas técnicas são utilizadas neste projeto e suas configurações e parâmetros estão nos Capítulos 05 e Anexos 1.

2.6. Integração de Sistemas Multiplataformas.

Há uma imensa variedade de aplicativos, dispositivos e equipamentos diferentes no mercado de automação industrial internacional, onde cada fabricante opta por um padrão de comunicação entre arquiteturas de sistemas (IEC, 2001). Mas com a difusão da rede mundial de computadores o mercado de automação industrial tende a adotar o TCP/IP como um protocolo padrão (CHENG ,1998).

Neste contexto este trabalho utiliza o serviço do protocolo de transferência de hipertexto (*HTTP*) cujo cliente da VPN acessa a área de serviço do servidor de internet.

O servidor de internet é o cliente da VPN local e acessa duas aplicações distintas em servidores de aplicações SCADA.

Assim pode-se administrar e controlar os experimentos no LCAP em processos químicos reais com similar interação do usuário local. A Figura 01 mostra a VPN na internet e a abertura de duas VPN's que foram criadas para o CRAPQ.

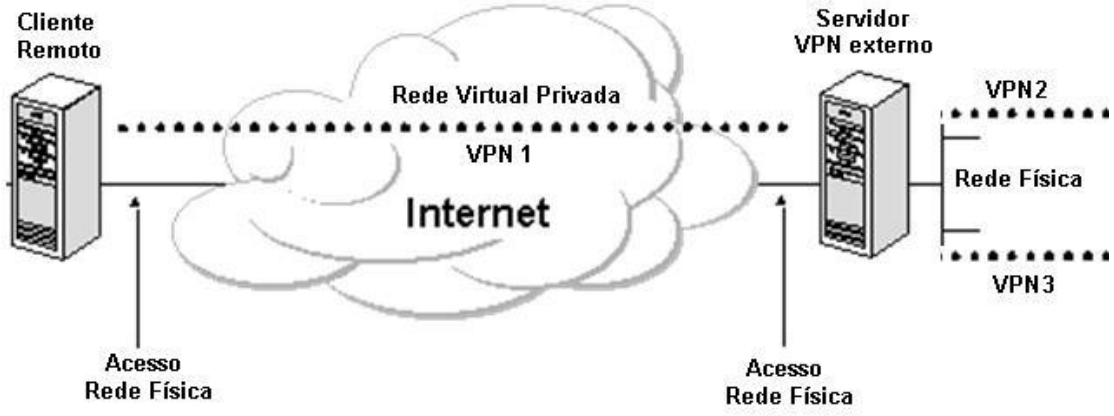


Figura 01. VPN na internet e VPN's no LCAP.

Os servidores de aplicações SCADA são acessados através de duas ferramentas, de utilização de licença livre (*Freeware*) que possuem técnicas de criptografia simétrica e assimétrica (SSH) alem de tunelamento de informação.

A compatibilidade com a máquina virtual JAVA, a criptografia assimétrica e o tunelamento de dados criam três VPN's que viabilizam todo trafego de informação segura entre duas ou mais máquinas independente do SIGE, SDCD, CLP, ou plataforma de sistema operacional, que operem estes servidores de aplicações SCADA.

Os pré-requisitos para configuração e instalação do PC que roda o cliente de internet e o PC que roda o servidor SCADA é que sejam compatíveis com o protocolo TCP/IP, possuam uma conexão física a internet e tenham navegadores de internet atuais (Internet Explorer®, Mozzila Firefox®, Opera®, etc).

As VPN's atualmente são as tecnologias mais eficazes e seguras de administração remota e usam o conceito de tunelamento de dados, cuja existência é anterior às VPN's.

O tunelamento pode ser definido como um processo de encapsulamento de um protocolo dentro de outro.

Nas VPN's além do tunelamento é incorporado um novo componente a esta técnica: antes de encapsular o pacote que será transportado, o mesmo é criptografado em 128 bits de forma a ficar ilegível caso seja interceptado durante o seu transporte (podendo ser criptografados em 256 bits).

O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e decriptografado, retornando ao seu formato original.

Uma característica importante é que os pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária (Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária).

Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada (KOMPELLA, 2006).

3. MATERIAIS E MÉTODOS.

3.1. Interfaces do Cliente de Internet e Cliente SCADA.

O CRAPQ faz a administração e o controle remoto de três sistemas distintos. As interfaces do usuário são acessadas da Internet ou na Intranet. Em ambos os casos o Cliente acessará os processos citados abaixo:

3.1.1 Protótipo Experimental para Conversão de Óleo Vegetal em Biodiesel.

O Caso-Estudo I, Sistema de Conversão de Óleo Vegetal em Biodiesel, instalado no LCAP detém parte dos Dispositivos Fieldbus (DI) do laboratório que foram analisados neste trabalho.

O reator multipropósito do Caso-Estudo I é composto pelos seguintes itens:

- Tanque de Etanol;
- Tanque de Fluido refrigerante (Água);
- Reator encamisado com capacidade de 500 mL;
- Bomba de re-circulação de Biodiesel;
- Bomba de re-circulação de fluído refrigerante;
- Inversor de freqüência para controle de velocidade do motor da bomba de fluído refrigerante;
- Inversor de freqüência para controle de velocidade do motor da bomba de biodiesel;
- Agitador Motorizado;
- Resistência de 400 W;
- Variador de tensão para resistência de aquecimento;
- Estação de trabalho SCADA I e II;
- Interface Fieldbus Distribuída (DFI);
- Dispositivos Inteligentes Fieldbus (DI). (Descritos a seguir).

A supervisão e o controle deste processo é realizado pelo DFI, após o DFI existem quatro Dispositivos Inteligentes Fieldbus (DI), onde três destes DI's são do modelo FI302 e um do modelo IF 302 .

Os modelos FI302 são os responsáveis pela aquisição de dados no campo de cinco Transmissores de Temperatura (TT).

Os TT's utilizados para a determinação de cinco temperaturas efetuam a medida nos seguintes pontos do reator multipropósito para o Caso Estudo I:

- Temperatura da entrada etanol;
- Temperatura da circulação de óleo vegetal;
- Temperatura da entrada do fluido refrigerante;
- Temperatura da saída do fluido refrigerante;
- Temperatura de reação no interior do reator.

A identificação nos três DI's do reator são representadas como FI303, FI304, FI305 e os TT's que adquirem cinco sinais das Pt100 instaladas nos equipamentos e tubulações estão identificados como, TT101, TT102, TT103, TT104, TT105.

O modelo IF 302 executa a função de um DI do tipo Conversor de Corrente que usa a variável manipulada (MV) do Bloco de Função PID ou de uma função Fuzzy-PID das aplicações Simulink ou Scicos.

A MV é um valor numérico gerado por uma das funções de controle em uso, o valor da MV é recebido no IF302 através de dados da rede digital Fieldbus (FFH1), assim que o IF302 recebe este valor da MV o converte em sinal analógico de 4-20 mA.

O sinal analógico é enviado ao inversor de freqüência previamente parametrizado, aumenta ou diminui a velocidade do motor na bomba de circulação de água conforme a amplitude deste sinal analógico refrigerando a camisa do reator do Caso Estudo I.

A representação do sistema SCADA acionado e monitorado pelo CRAPQ do Caso-Estudo I e seus dispositivos é mostrada na Figura 02.

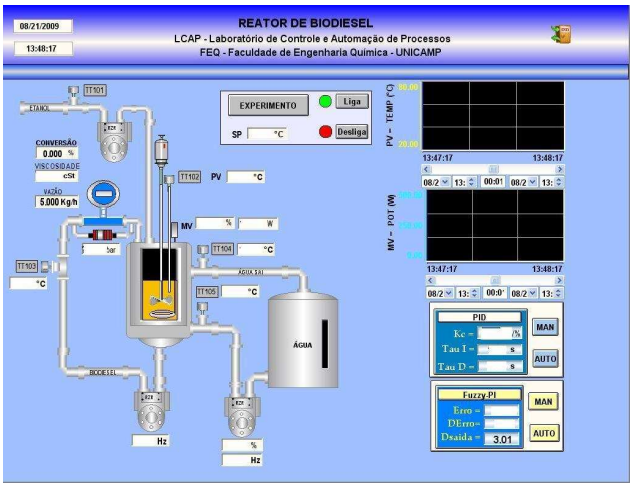


Figura 02. Sistema SCADA I do Caso-Estudo I.

3.1.2 Protótipo Experimental para Precipitação da Enzima do Abacaxi.

O Caso de Estudo II Sistema para Precipitação da Enzima do Abacaxi , instalado também no LCAP detém a outra parte dos Dispositivos Fieldbus (DI) do laboratório que também foram analisados neste trabalho.

O reator multipropósito do Caso-Estudo II é composto pelos seguintes itens:

- Reator encamisado com a capacidade 500 mL;
- Unidade de refrigeração de Propilenoglicol;
- Agitador motorizado com velocidade ajustável;
- Bomba de adição de etanol;
- Bomba de re-circulação do fluido refrigerante (propilenoglicol);
- Inversor de freqüência para controle da velocidade da bomba de fluído refrigerante;
- Estação de trabalho SCADA I e II;
- Interface Fieldbus Distribuída (DFI);
- Dispositivos Inteligentes Fieldbus (DI). (Descritos a seguir).

Neste Caso Estudo II a supervisão e o controle deste processo também é realizado pelo mesmo DFI do Caso Estudo I, mas nesta planta existem apenas três DI's, onde dois destes são do modelo FI302 e um do modelo IF 302.

Os modelos FI302 são os responsáveis pela aquisição de dados no campo de quatro Transmissores de Temperatura (TT).

Os TT's utilizados para a determinação das quatro temperaturas efetuam a medida nos seguintes pontos do reator multipropósito para o Caso Estudo II:

- Temperatura da entrada etanol;
- Temperatura de entrada do fluído refrigerante (propileno-glicol);
- Temperatura de saída do propileno-glicol;
- Temperatura de precipitação no interior do reator.

A aquisição dos dados de temperatura nos Caso Estudo I e II são através de termos-resistência do tipo pt100 devidamente calibradas para as condições do processo.

Os Sistemas de Controle de ambos reatores podem operar nos modos Automático e Manual. O modo Automático é gerenciado na lógica criada em Blocos de Função de controle.

A identificação nos dois DI's do reator do Caso Estudo I estão representadas como FI301, FI302, e os TT's que adquirem os quatro sinais das Pt100 instaladas nos equipamentos e tubulações estão identificados como, TT301, TT302, TT303, TT304.

O modelo IF 302 do reator do Caso Estudo II é idêntico ao do Caso Estudo I e possui as mesmas características de controle e funcionamento.

A supervisão do Caso Estudo II é também realizado pela mesma estação de trabalho do Caso Estudo I economizando a instalação de equipamentos e licenças de sistemas SCADA trabalho desenvolvido por SANTOS, 2006.

A representação do sistema SCADA II acionado e monitorado pelo CRAPQ do Caso-Estudo II e seus dispositivos é mostrada na Figura 03.

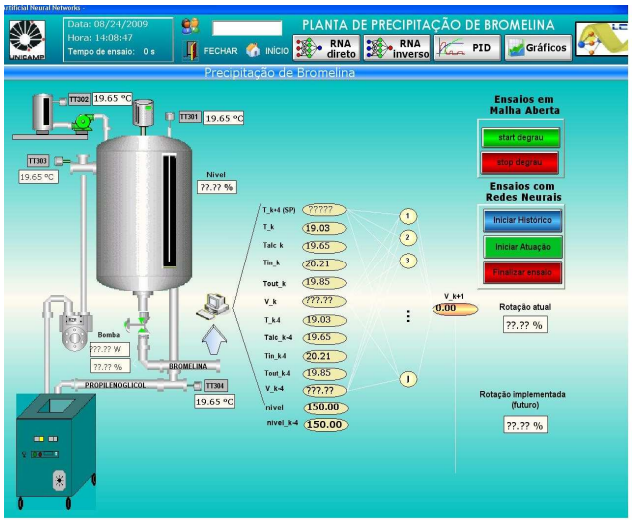


Figura 03. Sistema SCADA II do Caso-Estudo II.

3.1.3 Protótipo Experimental para estudo de Estratégias de Controle em um Sistema de Refrigeração de Liquido.

O Caso de Estudo III Sistema Refrigeração de Liquido, instalado em outra sala do LCAP possui um sistema de automação controlado por um Controlador Lógico Programável da Hi Tecnologia.

O do Caso-Estudo III é composto pelos seguintes itens:

- Compressor;
- Condensador;
- Evaporador;
- Ventilador;
- Válvulas de expansão;
- Torre de resfriamento de água;
- Trocador de calor casco e tubo;
- Bombas de deslocamento positivo;
- Resistências de aquecimento elétricas;
- Linha de abastecimento de água;
- Linha de abastecimento de propileno-glicol;

- Filtro de óleo;
- Filtro secador de refrigerante R22;
- Separador de Óleo;
- Separador de liquido;
- Visor de liquido;
- Pressostato diferencial;
- Sensores de pressão;
- Sensores de temperatura;
- Sensores de vazão;
- Inversor de frequência para controle de velocidade do compressor;
- Inversor de frequência para controle de velocidade da bomba;
- Estação de Trabalho SCADA II;
- Controlador Lógico Programável.

Por se tratar de uma planta com muitas variáveis de controle e muitas variáveis controladas não identificaremos os dados de aquisição de campo neste Caso Estudo III, para maiores informações do projeto completo pode ser consultado no trabalho de dissertação desenvolvido por Pinelli 2008.

A representação do sistema SCADA acionado e monitorado pelo CRAPQ do Caso-Estudo III e parte de seus dispositivos é mostrada na Figura 04.

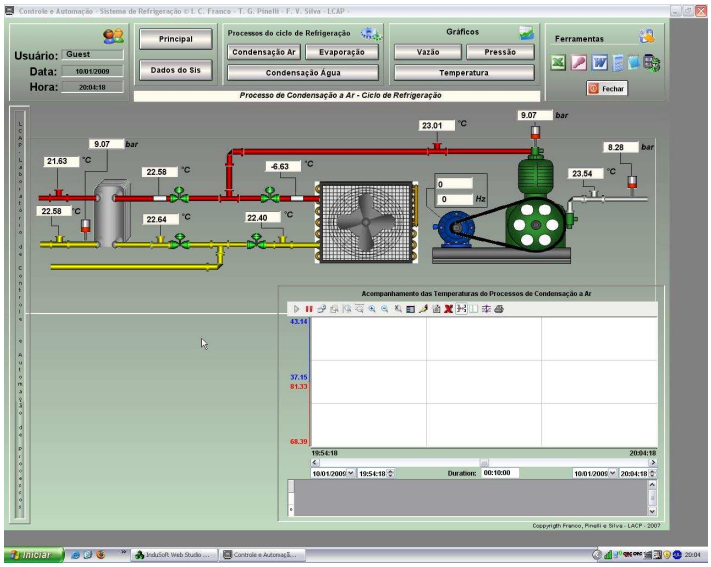


Figura 04. Sistema SCADA III do Caso Estudo III.

O CRAPQ foi projetado para acionar e monitorar todas aplicações indiferente de seus sistemas de automação, o local físico onde as plantas dos Caso Estudo I, II e III estão instaladas são mostrados nas Figuras 05 e 06.

Estes sistemas SCADA trabalham para as seguintes linhas de pesquisa:

- Desenvolvimento de pesquisa nas áreas de controle de processos de separação (destilação contínua e batelada) e sistemas reativos.
- Controle on-line de processos químicos através de sistemas industriais de controle on-line de processos químicos através de sistemas industriais de controle.
- Uso de técnicas de inteligência artificial em processos químicos.
- Refrigeração industrial e controle de ciclos frigoríficos.

Figura 05. DFI na Planta de Biodiesel e Bromelina

Figura 06.CLP na Planta de Refrigeração

Inicialmente, foi realizado um levantamento físico dos dispositivos e equipamentos para a determinação da configuração do Projeto Inicial.

3.1.4 Etapas preliminares para o desenvolvimento do Projeto do CRAPQ.

A determinação dos servidores e programas que construíram o formato inicial do projeto CRAPQ precedeu várias etapas até que fosse realizado o dimensionamento correto dos servidores e clientes, para a instalação e configuração dos equipamentos e programas segundo a compatibilidade dos PC's e equipamentos de informática do mercado. Os testes preliminares proveram à identificar os seguintes aspectos do sistema:

- O comportamento da comunicação LAN no servidor SCADA local;
- O comportamento da comunicação WAN no servidor de internet;
- A vulnerabilidade das VPN's abertas em cada host SCADA;
- A interoperabilidade entre aplicações dos sistemas SCADA;
- A versatilidade dos servidores continuarem operando após acontecer falhas de comunicação da LAN/WAN.
- A segurança dos dados que trafegam na rede mundial de computadores.

Os testes preliminares buscaram viabilizar o projeto principalmente para que as características de expansibilidade e interoperabilidade da arquitetura fossem funcionais, estritamente seguras e de fácil incorporação de novos projetos ao sistema.

A Figura 07 mostra a estrutura inicial proposta do CRAPQ em funcionamento no LCAP, onde os principais clientes e servidores do serviço são:

- Cliente de Internet WAN, equipamento (PC ou notebook) que acessa as aplicações SCADA através do Servidor de Internet;
- Cliente SCADA LAN, PC que acessa as três aplicações e simultaneamente executa o Servidor de Internet;

- Servidor de Internet, PC responsável por disponibilizar as três aplicações SCADA na internet por quatro áreas de trabalho diferentes;
- Servidor SCADA, PC responsável por disponibilizar a aplicação SCADA na rede LAN.

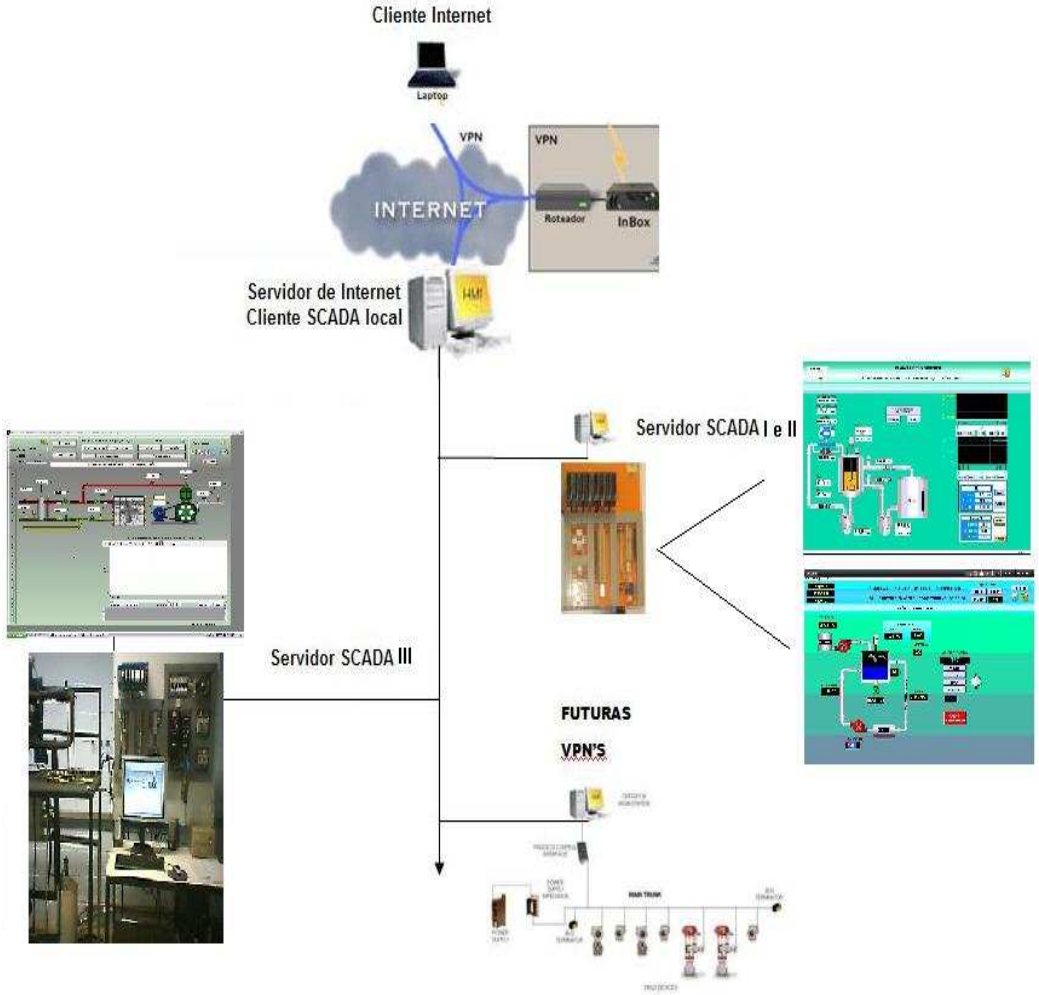


Figura 07. Estrutura proposta do CRAPQ.

3.2. Especificações do Servidor SCADA I e II.

Conforme a estrutura proposta na Figura 02 o desenvolvimento do CRAPQ requereu as seguintes especificações mínimas do Servidor SCADA I e II:

- Servidor *Complex Instruction Set Computer* – CISC (x86 Intel®);
- Processador Intel® Duo Core de 1.8 GHz (velocidade do *clock*);
- Disco rígido de 160 GB (capacidade de armazenamento);
- Memória *RAM* (*Random Access Memory*) com 1Gbyte (capacidade de armazenamento);
- Placa de rede padrão *Ethernet* 802.1;
- Sistema Operacional será Windows XP® Profissional SP7;
- Aplicação para Servidor de VPN instalada;
- Sistema SCADA previamente configurado.

3.3. Especificações do Servidor SCADA III.

Já o Servidor SCADA III foi dimensionado conforme a disposição física dos experimentos no laboratório requeria as seguintes especificações mínimas:

- Servidor *Complex Instruction Set Computer* – CISC (x86 Intel®);
- Processador Intel® Duo Core de 1.8 GHz (velocidade do *clock*);
- Disco rígido de 160 GB (capacidade de armazenamento);
- Memória *RAM* (*Random Access Memory*) com 1Gbyte (capacidade de armazenamento);
- Placa de rede sem fio padrão *Ethernet* 802.3;

- Sistema Operacional será Windows XP® Profissional SP7;
- Aplicação para Servidor de VPN instalada.
- Sistema SCADA previamente configurado.

3.4. Especificações do Servidor de Internet.

No Servidor de Internet a ser dimensionado o CRAPQ teve a flexibilidade para requerer as seguintes especificações mínimas:

- Servidor *Complex Instruction Set Computer* – CISC (x86 Intel®);
- Processador Intel® Duo Core de 1.8 GHz (velocidade do *clock*);
- Disco rígido de 160 GB (capacidade de armazenamento);
- Memória *RAM* (*Random Access Memory*) com 1Gbyte (capacidade de armazenamento);
- Placa 3D de 128 Mbyte.
- Sistema Operacional Linux ou Windows**.**
- Aplicação para Servidor de VPN WAN.
- Aplicação para comutação de terminal.
- Placa de rede padrão *Ethernet* 802.1 ou 802.3
- Sistema Operacional será Windows XP® Profissional SP7;
- Aplicação Cliente para serviços da VPN LAN.
- Sistema SCADA previamente configurado.

A especificação do Servidor de Internet e das configurações das aplicações envolvidas foi num primeiro momento para realizar os testes preliminares e verificar se havia viabilidade técnica para conclusão da especificação.

Assim posteriormente foi necessário realizar a alteração do projeto inicial devido à configuração preliminar não atender as condições técnicas necessárias para a comunicação entre a Intranet da Universidade e a Internet no Servidor de Internet.

3.5. Compatibilidade do Cliente de Internet ao CRAPQ.

Com base no projeto inicial do CRAPQ, descrito e ilustrado na proposta na Figura 07 e determinado pelos pré-requisitos do sistema anteriormente citados, foram dimensionados os equipamentos servidores e estações, para que as rotinas de acionamento e aquisição de dados realizadas no laboratório pudessem ser efetuadas a distância (remotamente). Neste contexto o Cliente de Internet são usuários externos, e os equipamentos e aplicações necessários para a interação com o CRAPQ foram dimensionados, para que este Cliente de Internet pudesse ter tecnologia compatível com os sistemas operacionais, navegadores e programas desenvolvidos em *JAVA® "Runtime Environment",* descritos a seguir:

- **Sistemas Operacionais:**

  Solaris® SPARC, Solaris® x86, Debian®, Kurumin® Linux, SUSE® Linux, Windows 98®, Windows ME®, Windows 2000® (SP2+), Windows XP® (SP2+), Vista®, Windows 2003®, JDS®, Windows Mobile CE®, Windows 7®.

- **Navegadores:**

  Internet Explorer® 5, Netscape® 4, Mozilla Firefox®1.4 ou versões superiores, Opera e Google Chrome.

- **JRE versão:**

  JVM 1.4.2 ou superior.

3.6. Etapas de instalação e configuração do Servidor de Internet.

Na Figura 08 é demonstrada a proposta do projeto inicial de configuração e parametrização do Servidor de Internet. Neste Servidor os Clientes das VPN locais são disponibilizados conforme as restrições de segurança, podendo abrir quatro Áreas de Serviço de Clientes Locais diferentes e com quatro ou mais Clientes Locais diferentes.

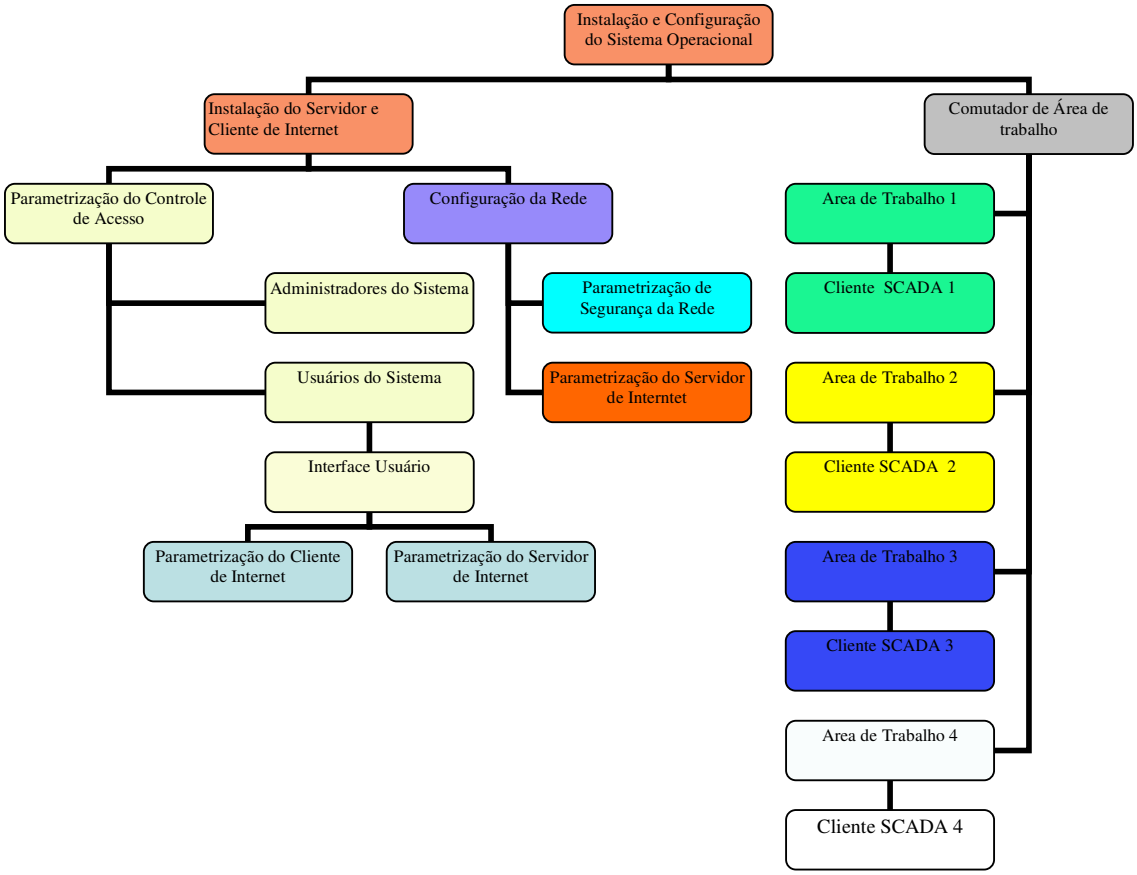


Figura 08 Parametrização e Configuração do Servidor de Internet.

3.7. Etapas de instalação e configuração dos Servidores SCADA I, II e III.

A proposta inicial para o funcionamento do CRAPQ nos Servidores SCADA I e II, disponibilizou executar as aplicações, configurações e gerenciamento dos dispositivos de automação como o Controlador Lógico Programável e a Interface Fieldbus Distribuída (CLP e DFI). Portanto os Servidores SCADA I, II e III disponibilizaram para o Servidor de Internet as telas obedecendo a parametrização das aplicações e sistemas envolvidos conforme demonstra o fluxograma na Figura 09.

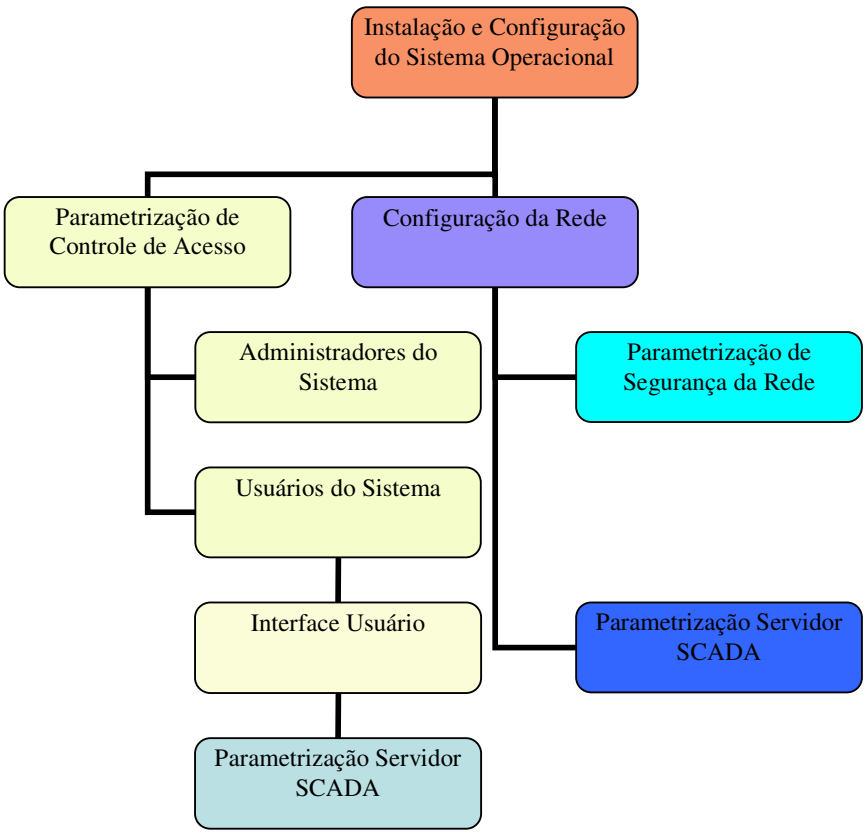


Figura 09 Parametrização e Configuração dos Servidores SCADA

3.8. Etapas de instalação e configuração dos Clientes.

A configuração do Navegador de Internet e a instalação do Cliente de VPN em computadores, "*notebooks*", habilitam o usuário do CRAPQ utilizar a interface do Cliente de Internet. E a instalação de Clientes de VPN em cartões de memória habilitará que usuários da Intranet possam utilizar o serviço dos Clientes SCADA da VPN local, como demonstra a Figura 10.

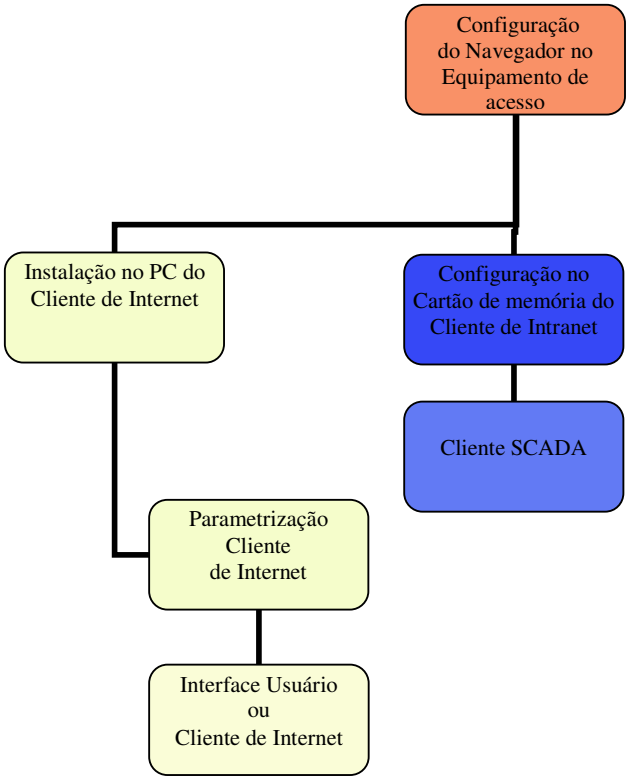


Figura 10. Parametrização e Configuração do Cliente de Internet.

3.9. Testes e análises preliminares.

Após o dimensionamento adequado do Projeto inicial CRAPQ, foi iniciada a fase de testes preliminares e a análise do sistema, com as aplicações FBViewer® Shark Analizer®.

O aplicativo FBViewer® verifica a taxa de transmissão entre os equipamentos FF® e dispositivos de campo FF®.

O programa Shark Analizer® é de uso gratuito, através da medição do tempo gasto entre o envio e recebimento de mensagens no protocolo TCP/IP. Foi possível determinar a operabilidade do CRAPQ medindo as taxas de transferência nos seguintes equipamentos e dispositivos (SHARPE, 2010):

- Interface Fieldbus Distribuída DFI.
- Dispositivo Conversor de Corrente FI;
- Dispositivo de Leitura de Corrente FI;
- CLP Hi®;
- Cliente de Internet;
- Ambiente Virtual;
- Servidor de Internet;
- Servidor SCADA I e II;
- Servidor SCADA III.

3.10 Análise dos quadros na rede High Speed Ethernet (HSE).

Através da execução do analisador de rede Ethernet (Shark-Analizer®) no Host SCADA, as mensagens (Quadros) enviadas e recebidas a o DFI foram capturadas e exportadas para uma planilha do Excel® nomeada como Planilha Ethernet (PETH).

Os quadros adquiridos na rede local e exportados para a planilha PETH, estão distribuídos em 22 tipos de protocolos de comunicação que são utilizados quando há solicitação de serviços das aplicações dos usuários de computadores no laboratório.

Apenas quatro protocolos são analisados neste trabalho que são: O Ethernet (ETH), Protocolo de Internet (IP), Protocolo de Controle e Transferência (TCP) e o Protocolo de Datagrama do Usuário (UDP).

A Tabela 01 mostra detalhadamente os campos dos Quadros transmitidos e capturados representando as Camadas padrão ISO/OSI.

Tabela 01. Dados dos Quadros HSE

Quadro	Serviços	Tamanho (bytes)
Enlace, Rede	ETH	14
Transporte	IP	20
Seção e Apresentação	UDP	8
Aplicação	UDP	51 a 400
Tamanho total do Quadro	UDP	93 a 442

As mensagens adquiridas totalizaram 20773 Quadros, onde uma amostra de 4121

quadros da planilha PETH foi retirada para ser o objeto de estudo.

3.11 Análise dos quadros na rede H1.

Simultaneamente a análise da rede HSE, foi executado o analisador de rede FF-H1 (FBView®). Os quadros enviados e recebidos na rede FF-H1 entre os Dispositivos Fieldbus e o DFI, nos processos de bateladas dos Casos-Estudo I e II foram exportados para outra planilha nomeada como Planilha FF-H1 (PFF-H1).

Na rede FF-H1 os quadros adquiridos estão distribuídos em 16 mensagens do Protocolo de Informação e Controle (PCI) gerenciados pelo agendador de barramento *"Link Active Scheduler"* (LAS).

O PCI provém serviços nas três subcamadas da Camada de Enlace (DLL) e utiliza o Protocolo de Dados Unitário (PDU) para ativar estes serviços em cada sub-camada. A Tabela 02 mostra detalhadamente a variação do tamanho dos quadros transmitidos na rede FF-H1 durante a análise, assim as Camadas não suprimidas ISO/OSI são comparadas as Camadas do padrão IEC 61158-2.

A Camada de Aplicação nem sempre envia dados de serviço (informação em bytes) a Camada de Especificação de Mensagem Fieldbus (FMS). Mas a informação dos

bytes ajustados são enviados a Sub-Camada de Acesso Fieldbus (FAS) que possui no mínimo 6 bytes de informação do PDU ajustados nesta camada. Portanto existe a variação no tamanho dos dados adquiridos na operação dos Reatores Multipropósito no Caso-Estudo I e II.

Tabela 02. Dados dos Quadros H1

Quadro	Serviços	Tamanho
Enlace	DLL / FAS / FMS	6 a 23 bytes
Aplicação	FMS PDU	0 a 251 bytes
Tamanho total do Quadro	DLL PDU	6 a 274 bytes

Os quadros adquiridos pelo analisador de rede totalizaram 229887, onde extraíram-se dados de aproximadamente 1/8 da amostra total, que consistiu uma fração de 45976 quadros. Considerando que o comportamento desta fração foi suficiente para demonstrar o comportamento geral da amostra pela atividade apresentada no instante de funcionamento das aplicações, pois ao analisar amostra total dividida em oito períodos, pode se notar uma atividade relativamente similar durante o ensaio total. Devido a dificuldade de filtrar os quadros que tramitaram ponto a ponto foi utilizado esta fração da amostra para assim gerar a planilha PFF-H1 que serviu de base neste estudo.

Com base nos dados das planilhas PFF-H1 e PETH foi explicada a correlação entre o trabalho de comunicação das duas redes e os Dispositivos Inteligentes de Campo.

Após realizados os testes nas instalações preliminares de equipamentos, aplicações e de comunicação na rede LAN e rede WAN, foi possível determinar os componentes necessários para projeto inicial do CRAPQ. Analisado então: os componentes, a estrutura proposta, a relação entre o equipamento físico e as aplicações, foram direcionados os equipamentos e soluções de aplicações que estão descritas nas Tabela 03 e 04 que formaram o Projeto Inicial do CRAPQ. Assim foram configuradas as seguintes funções dos equipamentos no sistema: o tipo de computador, os equipamentos de informática, aplicações de abertura de VPN´s.

Tabela 03 - Descrição da Configuração do Projeto Inicial CRAPQ.

CONFIGURAÇÃO	
Computadores	
Função	**Arquitetura**
Servidor de Internet	RISC / Desktop
Servidor SCADA 1	CISC / Desktop
Servidor SCADA 2	CISC / Desktop
Cliente SCADA local 1	CISC / Desktop
Cliente SCADA local 2	CISC / Desktop
Cliente de Internet	CISC / Desktop ou Laptop

Tabela 04 – Descrição Geral do Projeto Inicial CRAPQ.

DESCRIÇÃO GERAL	
Equipamnetos	
Função	**Tipo**
Interface FF-H1 e Ethernet	Comutador ETH 100 Mbps
Interface de rede local para sem fio	Roteador de rede sem fio 100 Mbps
Interface de rede local	Placa de rede Ethernet
Sistemas Operacionais	
Função	**Tipo**
Servidor de Internet	Linux Debian® ou Kurumin®
Servidor SCADA I e II	Windows XP®
Servidor SCADA III	Windows XP®
Cliente SCADA local I e II	Linux Debian® ou Kurumin®
Cliente SCADA local III	Linux Debian® ou Kurumin®
Cliente de Internet	WindowsXP®,Linux,CE®
Aplicações	
Função	**Tipo**
Servidor de Internet	OpenVPN®, NXServer®,TigthVNC®
Servidor SCADA I e II	OpenVPN®, NXServer®,TigthVNC®
Servidor SCADA III	OpenVPN®, NXServer®,TigthVNC®
Cliente SCADA local I e II	OpenVPN®, NXServer®,TigthVNC®
Cliente SCADA local III	OpenVPN®, NXServer®,TigthVNC®
Cliente de Internet	OpenVPN®, NXServer®,TigthVNC®

Nos testes preliminares de comunicação e de funcionamento dos equipamentos e dos aplicativos as discussões e conclusões levaram a reformulação do Projeto Inicial fazendo com que o Projeto Final do CRAPQ direcionasse aos Equipamentos e Soluções propostas descritas na Tabela 05.

3.12 Reestruturação da Instalação.

A realidade dos problemas de viabilidade técnica e de funcionamento do meio físico, identificados no Projeto Inicial e a reestruturação da instalação do CRAPQ deu um novo panorama para a mudança da arquitetura anteriormente proposta. Neste novo panorama foi proposto para a seguinte arquitetura do Sistema de Controle Remoto para Automação de Processos Químicos como mostrado nas Tabelas 05 e 06.

Tabela 05 – Descrição da Configuração do Projeto Final do CRAPQ.

CONFIGURAÇÃO	
Computadores	
Função	**Arquitetura**
Servidor de Internet	CISC / Desktop
Servidor SCADA I e II	CISC / Desktop
Servidor SCADA III	CISC / Desktop
Cliente SCADA local I e II	CISC / Desktop
Cliente SCADA local III	CISC / Desktop
Cliente de Internet	CISC / Desktop ou Laptop
Equipamentos	
Função	**Tipo**
Interface FF-H1 e Ethernet	Comutador ETH 100 Mbps
Interface de rede local para sem fio	Roteador de rede sem fio 100 Mbps
Interface de rede local	Placa de rede Ethernet

Tabela 06 – Descrição dos Programas do Projeto Final do CRAPQ.

PROGRAMAS	
Sistemas Operacionais	
Função	**Tipo**
Servidor de Internet	Windows XP® Professional
Servidor SCADA I e II	Windows XP® Professional
Servidor SCADA III	Windows XP® Professional
Cliente SCADA local I e II	Windows XP® Professional
Cliente SCADA local III	Windows XP® Professional
Cliente de Internet	WindowsXP®, Debian ,Kurumin ,Windows CE®
Aplicações	
Função	**Tipo**
Servidor de Internet	LogMeIn®, Tigth VNC®, Yod'm 3D®
Servidor SCADA I e II	Tigth VNC®
Servidor SCADA III	Tigth VNC®
Cliente SCADA local I e II	Tigth VNC®
Cliente SCADA local III	Tigth VNC®
Cliente de Internet	LogMeIn®

Nota-se que houve mudanças significativas nas entre o Projeto Inicial e o Projeto Final, principalmente relacionado ao Servidor de Internet e o Cliente de Internet, devido a inviabilidade de obtenção de uma porta especifica para a VPN, foi necessário configurar o sistema com programas (Freeware) que trabalham em protocolo HTTP criptografado (Logmein®) e para uma maior compatibilidade com esta configuração foi necessário a troca do Sistema Operacional de Linux para Microsoft®.

Os resultados das análises e discussões são demonstrados através de expressões que são atribuídas em Análise Temporal de Algoritmos (HOROWITZ e SAHNI, 1978).

O mapeamento das configurações do projeto são mostradas num Diagrama de Caso de USO (UML) e as configurações das aplicações como Tigth VNC® Server e Viewer, Logmein® do CRAPQ estão no final nos Anexo 1, Anexo 2, Anexo 3 e Anexo 4.

3.13 Testes finais entre Cliente SCADA Local I e II, Servidor SCADA I e II.

Os testes realizados entre o Servidor SCADA e o Cliente SCADA foram obtidos das seguintes expressões:

- Tempo de Estabelecimento de Conexão SCADA (TEC-I);
- Tempo de Inicialização do Cliente SCADA (TIC-l);
- Tempo de Resposta do Dispositivo de Entrada do Cliente SCADA (TRD-I);
- Tempo de Atualização de Vídeo do Cliente SCADA (TAV-I);
- Tempo de Inicialização de Programas no Servidor SCADA (TIP-I);
- Taxa de Utilização da Rede Local pelo Cliente e Servidor SCADA (TUR-I);

TEC-I:

O Tempo de Estabelecimento de Conexão na rede local é medido pela Equação 1.0

$$TEC = \left(2 \times \left(\sum_{n\geq 1}^{i} TiEntA_n + \sum_{n\geq 1}^{i} TiCompA_n + \sum_{n\geq 1}^{i} TiSaidaA_n \right) + \sum_{n\geq 1}^{i} TiTransf_n \right) + \left(\sum_{n\geq 1}^{i} TiEntB_n + \sum_{n\geq 1}^{i} TiCompB_n + \sum_{n\geq 1}^{i} TiSaidaB_n + \sum_{n\geq 1}^{i} TiTransf_n \right) \quad (1.0)$$

A expressão mostrada na Equação 1.0 mede o Tempo de Acionamento do Dispositivo de Entrada (TiEnt), o Tempo de Computação do Dispositivo (TiComp), o Tempo de Saída do Dispositivo (TiSaida) e o Tempo de Transferência de dados na rede (TiTransf). Onde o Dispositivo de Entrada pode ser o mouse, teclado ou placa de rede, e o Dispositivo de Saída o monitor e a placa de rede. O Tempo de Computação do Dispositivo se refere ao tempo gasto pelos processos iniciados no Equipamento. E "A" ,"B"... "Z" são atribuídos a cada Dispositivo que faz parte do sistema.

O primeiro termo da equação referente ao Dispositivo "A" é multiplicado por dois considerando que TiEnta, TiCompa e TiSaidaa executam a mesma operação no momento da transmissão e da recepção devido o acionamento do Dispositivo de Entrada partir deste Dispositivo. O Dispositivo "B" executa a operação de recepção e transmissão sem que haja acionamento de um Dispositivo de Entrada como teclado e mouse, por isso é calculado somente uma vez. Considerando que o Equipamento "A" é o Cliente SCADA – I e II que é inicializado na Área de Serviço – I do Equipamento "B" (Servidor de Internet) .

TIC-l:

O Tempo de Inicialização do Cliente SCADA no Servidor de SCADA na rede local é medido pela Equação 1.1.

$$TIC - I = \sum_{n\geq 1}^{i} TiEntB_n + \sum_{n\geq 1}^{i} TiCompB_n + \sum_{n\geq 1}^{i} TiSaidaB_n \qquad (1.1)$$

Na Equação 1.1 é medida a Inicialização do Cliente SCADA após o estabelecimento de conexão entre o Cliente SCADA e o Servidor SCADA.

TRD-I:

Este teste mediu o Tempo de Resposta do Dispositivo de Entrada do Cliente SCADA em relação ao Servidor SCADA dado na Equação 1.2.

$$TRD-I=\left(2\times\left(\sum_{n\geq1}^{i}TiEntA_n+\sum_{n\geq1}^{i}TiCompA_n+\sum_{n\geq1}^{i}TiSaidaA_n\right)+\sum_{n\geq1}^{i}TiTransf_n\right)+\left(\sum_{n\geq1}^{i}TiEntB_n+\sum_{n\geq1}^{i}TiCompB_n+\sum_{n\geq1}^{i}TiSaidaB_n+\sum_{n\geq1}^{i}TiTransf_n\right) \quad (1.2)$$

TAV-I:

O tempo de Atualização de Vídeo do Cliente SCADA mediu a atualização de regiões de vídeo mapeadas no Servidor SCADA. Este tempo foi obtido pela Equação 1.3

$$TAV-I=\left(\sum_{n\geq1}^{i}TiEntB_n+\sum_{n\geq1}^{i}TiCompB_n+\sum_{n\geq1}^{i}TiSaidaB_n\right)+\sum_{n\geq1}^{i}TiTransfn+\left(\sum_{n\geq1}^{i}TiEntA_n+\sum_{n\geq1}^{i}TiCompA_n+\sum_{n\geq1}^{i}TiSaidaA_n\right) \quad (1.3)$$

TIP-I:

A Equação 1.4 faz a somatória do tempo de inicialização de programas no Servidor SCADA medido a partir da solicitação do Equipamento “A” (Cliente SCADA I).

$$TIP-I=\left(2\times\left(\sum_{n\geq1}^{i}TiEntA_n+\sum_{n\geq1}^{i}TiCompA_n+\sum_{n\geq1}^{i}TiSaidaA_n\right)+\sum_{n\geq1}^{i}TiTransf_n\right)+\left(\sum_{n\geq1}^{i}TiEntB_n+\sum_{n\geq1}^{i}TiCompB_n+\sum_{n\geq1}^{i}TiSaidaB_n+\sum_{n\geq1}^{i}TiTransf_n\right) \quad (1.4)$$

TUR-I:

A taxa de utilização da rede local é medida pela somatória dos tempos de transmissão durante as operações na rede local de todas as Equações anteriores expressas na Equação 1.5.

$$TUR-I=\left(\begin{array}{l} TEC\sum_{n\geq 1}^{i}TiTransf_n+TRD-I\sum_{n\geq 1}^{i}TiTransf_n+ \\ TAV-I\sum_{n\geq 1}^{i}TiTransf_n+TIP-I\sum_{n\geq 1}^{i}TiTransf_n \end{array}\right) \qquad (1.5)$$

3.14 Testes finais entre Cliente SCADA Local III e Servidor SCADA III.

Os testes realizados entre o Servidor SCADA III e o Cliente SCADA III foram obtidos das seguintes expressões:

- Tempo de Estabelecimento de Conexão SCADA – III (TEC-II);
- Tempo de Inicialização do Cliente SCADA III (TIC-II);
- Tempo de Resposta do Dispositivo de Entrada do Cliente SCADA III (TRD-II);
- Tempo de Atualização de Vídeo do Cliente SCADA III (TAV-II);
- Tempo de Inicialização de Programas no Servidor SCADA III (TIP-II);
- Taxa de Utilização da Rede Local pelo Cliente e Servidor SCADA III (TUR-II);

TEC-II:

O Tempo de Estabelecimento de Conexão na rede local é medido pela Equação TEC – II idêntica a Equação 1.0.

A Equação TEC - II mede o Tempo de Estabelecimento de Conexão que usa termos iguais aos da Equação 1.0 considerando que o Equipamento “A” neste caso é o Cliente SCADA – III que é inicializado na Área de Serviço – II do Equipamento “B” (Servidor de Internet). Servindo como regra para as equações subseqüentes.

TIC-II:

O Tempo de Inicialização do Cliente SCADA III no Servidor de SCADA III na rede local é medido pela Equação 1.1.

Na Equação 1.1 é medida a Inicialização do Cliente SCADA III após o estabelecimento de conexão entre o Cliente SCADA III e o Servidor SCADA III.

TRD-II:

Este teste mediu o Tempo de Resposta do Dispositivo de Entrada do Cliente SCADA III em relação ao Servidor SCADA III dado na Equação 1.2.

TAV-II:

O tempo de Atualização de Vídeo do Cliente SCADA III mediu a atualização de regiões de vídeo mapeadas no Servidor SCADA III. Este tempo foi obtido pela Equação 1.3.

TIP-II:

A Equação 1.4 faz a somatória do tempo de inicialização de programas no Servidor SCADA III medido a partir da solicitação do Equipamento “A1” (Cliente SCADA II).

TUR-II:

A taxa de utilização da rede Local é medida pela somatória dos tempos de transmissão durante as operações na rede local de todas as Equações anteriores expressa na Equação 1.5.

3.15 Testes finais entre Cliente de Internet e Servidor de Internet.

O Cliente de Internet onde os testes foram realizados, situa-se na cidade de Santo André, a mais de 120 km de distância do Servidor de Internet. Este cliente devidamente instalado e parametrizado em um computador. Pode-se optar à trabalhar com três Sistemas Operacionais e quatro versões de Navegadores de Internet. Os Sistemas Operacionais que podem ser usados pelo Cliente de Internet são:

- Windows XP® Professional SP5 – Sistema da Microsoft Systems;
- Kurumin® Linux 7 – Sistema baseado em Unix de Código Aberto desenvolvido por Carlos Yamamoto;
- Debian® Lenny 6 – Sistema Operacional baseado em Unix de Código Aberto por DEBIAN®.

Os testes realizados entre o Servidor de Internet e o Cliente de Internet utilizaram as seguintes medidas:

- Tempo de Estabelecimento de Conexão Ambiente Virtual (TEC – III) idem Equação 1.0;
- Tempo de Estabelecimento de Conexão ao Servidor de Internet (TEC – IV) idem Equação 1.0;
- Tempo de Inicialização do Acesso ao Sistema Operacional (TIO) Equação 1.6;
- Tempo de Estabelecimento de Conexão ao Servidor SCADA I e II pelo Cliente de Internet (TEC – V) idem Equação 1.0;

- Tempo de Resposta do Dispositivo de Entrada do Cliente Internet (TRD - III) idem Equação 1.2;
- Tempo de Comutação de Área de Serviço I para II (TCA) Equação 1.7;
- Tempo de Estabelecimento de Conexão ao Servidor SCADA III pelo Cliente de Internet (TEC- VI) idem Equação 1.0;
- Tempo de Resposta do Dispositivo de Entrada do Cliente Internet (TRD – V) idem Equação 1.2;
- Tempo de Atualização de Vídeo do Cliente de Internet (TAV - III) idem Equação 1.3;
- Tempo de Atualização de Vídeo do Cliente de Internet (TAV - IV) idem Equação 1.3;
- Tempo de Inicialização de Programas no Servidor SCADA I e II (TIP-III) idem Equação 1.4;
- Tempo de Inicialização de Programas no Servidor SCADA III (TIP-IV) idem Equação 1.4;
- Taxa de Utilização da Rede Local pelo Cliente e Servidor de Internet (TUR-II) idem Equação 1.5.

TEC – III:

O Tempo de Estabelecimento de Conexão na Internet é medido pela Equação TEC – III.

A Equação TEC - III neste caso mede o Tempo de Estabelecimento de Conexão ao ambiente virtual que é iniciado a partir da identificação de usuário e senha do Cliente de Internet.

Na Equação TEC -III é usado termos iguais as expressões da Equação 1.0 e da Equação TEC - III, porém considera-se que o Equipamento "A" neste caso é o Cliente de Internet (computador remoto) que é inicializado no Ambiente Virtual (Proxy de Internet do LogMeIn®). Servindo como regra para as equações subseqüentes.

TEC – IV:

O Tempo de Estabelecimento de Conexão na Internet é medido pela Equação TEC – IV idêntica a Equação 1.0.

A Equação TEC - IV mede o Tempo de Estabelecimento de Conexão ao Servidor de Internet que é iniciado a partir da identificação de usuário e senha do Cliente de Internet ao Sistema Operacional no Servidor de Internet.

Na Equação considera-se que o Equipamento "A" neste caso é o Cliente de Internet (estação remota) que é inicializado no Equipamento "B" (Servidor de Internet).

TIO:

O Tempo de Inicialização do Acesso ao Sistema Operacional é expresso pela Equação 1.6.

$$TIO = \left(2 \times \left(\sum_{n\geq 1}^{i} TiEntA_n + \sum_{n\geq 1}^{i} TiCompA_n + \sum_{n\geq 1}^{i} TiSaidaA_n \right) + \sum_{n\geq 1}^{i} TiTransf_n \right) + \left(\sum_{n\geq 1}^{i} TiEntB_n + \sum_{n\geq 1}^{i} TiCompB_n + \sum_{n\geq 1}^{i} TiSaidaB_n + \sum_{n\geq 1}^{i} TiTransf_n \right) \quad (1.6)$$

A Equação 1.6 mede o TIO a partir da solicitação de usuário e senha feita pelo Sistema Operacional ao Equipamento "A" que neste caso é o Cliente de Internet (estação remota) e o Equipamento "B" o Servidor de Internet.

TEC – V:

O TEC - V é medido através Equação 1.0

A TEC – V mede o Tempo de Estabelecimento de Conexão ao Servidor de Internet que é iniciado a partir da identificação de usuário e senha do Cliente de Internet ao Servidor SCADA I e II na Área de Serviço I do Servidor de Internet.

Na Equação 1.0 considera-se que o Equipamento "A" neste caso é o Cliente de Internet (estação remota) que é inicializado no Equipamento "B" Servidor de Internet e o Equipamento "C" o Servidor SCADA - I.

TRD - III:

O TRD - III é medido entre o Cliente de Internet com relação ao Servidor SCADA I dado na Equação 1.2.

TCA:

O TCA é medido entre o Cliente de Internet com relação ao Servidor de Internet dado na Equação 1.7.

$$TCA = \left(2 \times \left(\sum_{n\geq 1}^{i} TiEntA_n + \sum_{n\geq 1}^{i} TiCompA_n + \sum_{n\geq 1}^{i} TiSaidaA_n \right) + \sum_{n\geq 1}^{i} TiTransf_n \right) + \left(\sum_{n\geq 1}^{i} TiEntB_n + \sum_{n\geq 1}^{i} TiCompB_n + \sum_{n\geq 1}^{i} TiSaidaB_n + \sum_{n\geq 1}^{i} TiTransf_n \right) \quad (1.7)$$

A expressão da Equação 1.7 considera os mesmos Equipamentos da Equação 1.0.

TEC - VI:

O TEC - VI é medido através Equação 1.0.

TRD – V:

O TRD – V é medido entre o Cliente de Internet com relação ao Servidor SCADA II dado na Equação 1.2.

TAV - III:

O tempo de Atualização de Vídeo do Cliente de Internet mediu a atualização de regiões de vídeo mapeadas no Servidor SCADA I e II. Este tempo foi obtido pela Equação 1.3.

TAV - IV:

O tempo de Atualização de Vídeo do Cliente de Internet mediu a atualização de regiões de vídeo mapeadas no Servidor SCADA III. Este tempo foi obtido pela Equação 1.3.

TIP-III:

A Equação 1.4 faz a somatória do tempo de inicialização de programas no Servidor SCADA III medido a partir da solicitação do Equipamento “A1” (Cliente SCADA III).

TIP-IV:

A Equação 1.4 faz a somatória do tempo de inicialização de programas no Servidor SCADA III medido a partir da solicitação do Equipamento “A1” (Cliente SCADA III).

TUR-II:

A taxa de utilização da rede Local é medida pela somatória dos tempos de transmissão durante as operações na rede local de todas as Equações anteriores expressa na Equação 1.5.

3.16 Teste de captura de dados transferidos na VPN do CRAPQ.

Os dados enviados de comandos operados em dispositivos de entrada (mouse e teclado) e os dados recebidos de comandos para execução em dispositivos de saída (monitores e telas de dispositivos móveis) tratam de informações confidenciais do CRAPQ.

Para verificar a ilegibilidade de um dado transmitido foi utilizado o analisador de rede Shark Analizer® para ler um dado que trafega na rede entre o Cliente de Internet e o Servidor SCADA III.

O computador espião foi uma máquina no LCAP instalada ao lado do Servidor SCADA III que capturou o dado que trafegava no momento da operação do Cliente de Internet ao Servidor SCADA III.

Como o Computador espião e o Servidor SCADA III estavam sob as seguintes condições: na mesma intranet, no mesmo roteador, terem os endereços de internet identificados, e o mapeamento completo ponto a ponto do Cliente de Internet ao Servidor SCADA III, foi possível capturar o dado e seu conteúdo no momento exato de chegada da ordem enviada pelo Cliente de Internet ao Servidor SCADA III e sua resposta no momento exato da ordem de atualização no Cliente de Internet.

Os resultados deste item e dos anteriores são pauta de discussão da seção posterior, portanto não demonstrado nesta seção. Foram omitidos detalhes de configuração da maquina espiã, pois o objetivo desta foi apenas utilizá-la como ferramenta de detecção de dados entre dois computadores na internet, após a captura do dado a máquina foi desativada e suas configurações não documentadas por questões de segurança.

4. RESULTADOS E DISCUSSÕES.

Neste capítulo serão apresentados os resultados obtidos nos ensaios realizados com o CRAPQ operando os Servidores SCADA I, II e III local e a distância. Segue-se a estes as discussões pertinentes ao observado em cada situação.

Após a determinação da configuração foram realizados diversos ensaios de comunicação com base nesta configuração inicial para o CRAPQ, já mostrados na Tabela 1. Nos ensaios de comunicação foram identificados os seguintes problemas da configuração
do Projeto Inicial que são demonstrados na Tabela 07.

Tabela 07 – Resultado de testes dos computadores e equipamentos do projeto inicial CRAPQ.

Resultado de Teste Preliminar	
Computadores	
Função	**Conclusão de funcionamento**
Servidor de Internet	Estável
Servidor SCADA I e II	Estável
Servidor SCADA III	Estável
Cliente SCADA local I e II	Estável
Cliente SCADA local III	Estável
Cliente de Internet	Estável
Equipamentos	
Função	**Conclusão de funcionamento**
Interface FF-H1 e Ethernet	Estável
Interface de rede local sem fio	não existente
Interface de rede local	Estável

Tabela 08 – Resultado de teste de sistemas operacionais e aplicações do projeto inicial CRAPQ.

Sistemas Operacionais	
Função	**Conclusão de funcionamento**
Servidor de Internet	Estável
Servidor SCADA I e II	Estável
Servidor SCADA III	Estável
Cliente SCADA local I e II	Estável
Cliente SCADA local III	Estável
Cliente de Internet	Estável

Aplicações	
Função	**Resultado de Teste Preliminar**
Servidor de Internet	sem comunicação
Servidor SCADA I e II	Estável
Servidor SCADA III	Estável
Cliente SCADA local I e II	Estável
Cliente SCADA local III	sem comunicação
Cliente de Internet	sem comunicação

Após os testes preliminares realizados na arquitetura e na configuração do projeto inicial foi identificado um problema no meio físico utilizado pelo CRAPQ (sem dispositivos de rede sem fio), e um segundo problema relacionado a viabilidade do projeto como um todo (ausência de porta exclusiva para VPN).

Como pode ser observado nos resultados preliminares obtidos na Tabela 07 e 08 houve a necessidade de mudar toda estratégia de arquitetura dos sistemas operacionais e aplicações que formavam o Projeto Inicial. Principalmente devido o problema relacionado ao Cliente de Internet e o Servidor de Internet, cuja configuração da porta de VPN exclusiva para o Servidor de Internet no Servidor Coorporativo, foi limitada a um número determinado de portas, assim não havia disponibilidade para a reserva deste tipo de porta exclusiva para o projeto. Este problema tornaria o projeto inviável do ponto de vista técnico. Assim, a reestruturação desta arquitetura de sistemas operacionais e aplicações para a especificação e instalação do CRAPQ foi mudada para que o projeto fosse desenvolvido com sucesso.

Os dois problemas do meio físico eram:

- A instabilidade de comunicação da Rede FF-HSE no Servidor SCADA I e II.
- A ausência da porta de comunicação exclusiva pelo Servidor coorporativo devido o uso de portas padrão para o protocolo de datagrama unitário (UDP) e o protocolo de hiper texto (HTTP).

4.1 Testes das redes de comunicação FF-H1, HSE, Ethernet.

4.1.1 A instabilidade de comunicação FF-H1 e HSE.

Os casos-estudo I e II acessados pelo Cliente SCADA local I e II apresentaram falhas de comunicação entre o Servidor SCADA I e II e os Dispositivos Inteligentes de Campo (DI) controlados pelo Dispositivo de Interface Fieldbus (DFI). A análise de rede realizada com o aplicativo de gerenciamento de rede Shark-Analizer® não apresentou ruído ou erro de comunicação no envio e resposta das mensagens nas placas de rede no Servidor SCADA I e no DFI.

A identificação do problema de comunicação entre o Cliente SCADA local I e II, o Servidor SCADA I e II, e os DI's se deu quando foi levantada a suspeita de que não bastava verificar o trafego de mensagens na rede entre estes pontos, mas que seria estritamente necessária a medição do sinal físico eletrônico na rede FF-H1. Assim foi feita a medição com um osciloscópio que pode mostrar a interferência dos sistemas de disparo nos inversores de freqüência quando estavam em operação nos Caso-Estudo I e II. O ruído gerado pelo circuito de disparo dos inversores de frequência era suficiente para que o DFI não conseguisse distinguir a informação de dados dos instrumentos DI instalados nos caso-estudo I e II. Assim o ruído ocasionava a perda de informação para o Servidor SCADA I e II consequentemente ocasinava a ausência de informação no Cliente SCADA local I e II, por este motivo o analisador de rede não identificou problema na rede HSE.

Após a identificação do problema na rede FF-H1 foram tomadas duas providências para que o CRAPQ pudesse ser desenvolvido sem erros de leitura no campo; as providencias foram:

- Refazer a malha de aterramento dos instrumentos e DI instalados nos Casos-Estudo;
- Instalar o terminador de rede no final da FF-H1.

Assim as malhas de aterramento nos reatores foram normalizadas e o terminador de rede Fieldbus Foundation foi instalado normalizando a instabilidade de comunicação.

4.1.2 Resultados do sistema FF aplicado a reatores multipropósito.

Os locais de rede onde os quadros analisados e tratados nas planilhas PETH e PFFH1 trafegaram durante o funcionamento dos Casos-Estudo I e II foram classificados em quatro categorias que são:

- Dispositivos FF-H1 (DFF-H1) instalados nos Reatores Multipropósito I e II.

- Dispositivo de Interface Fieldbus (DFI) onde é feito a interface e configuração das redes FF-H1 e HSE;
- Supervisor (SUP) onde funcionam o Supervisórios SCADA e os Controladores Avançados.
- Área de Rede Local (LAN) ambiente de rede local onde a rede HSE e Ethernet local coexistiam, cuja conexão física é feita entre: o computador do SUP , 6 computadores de usuários da internet e uma impressora de rede, através de um comutador de 17 portas 10 Mbps.

Na Tabela 09 mostra o número de quadros transmitidos em cada categoria, o total da amostra de quadros analisados, o tempo total gasto pelos quadros da origem até o destino conforme amostra estudada.

Tabela 09. Local da medição de rede, numero de quadros e tempo médio.

Local	Numero de Quadros	Tempo Médio (s)
LAN	4121	0,0863639
DFFH1	45976	0,006
SUP para DFI	1503	0,1808760
LAN + SUP + DFFH1	50097	--------

A análise do comportamento na rede LAN cuja amostra de 4121 quadros Ethernet, obtiveram o intervalo de tempo de envio e recebimento dos quadros padrão Ethernet de 0,02 a 0,028 segundos, como mostra a Figura 11.

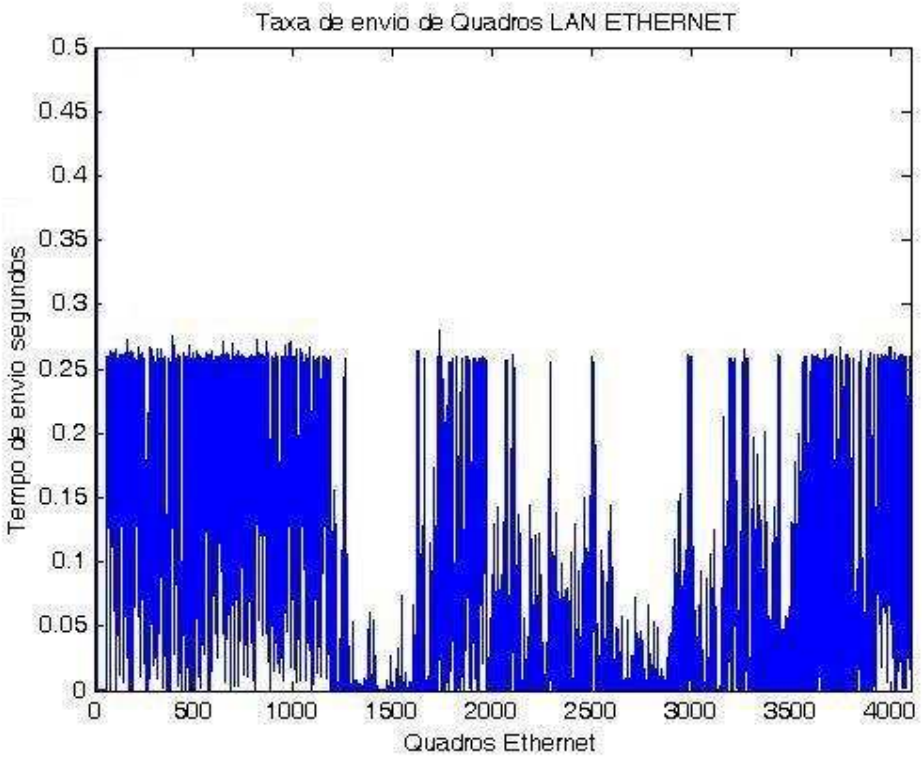


Figura 11. Comportamento padrão Ethernet.

Neste mesmo meio físico os quadros enviados pela rede FF-HSE totalizaram 1503 quadros que obtiveram o intervalo de tempo de envio e recebimento dos quadros padrão HSE de 0,13 a 0,26 segundos, conforme ilustra a Figura 12.

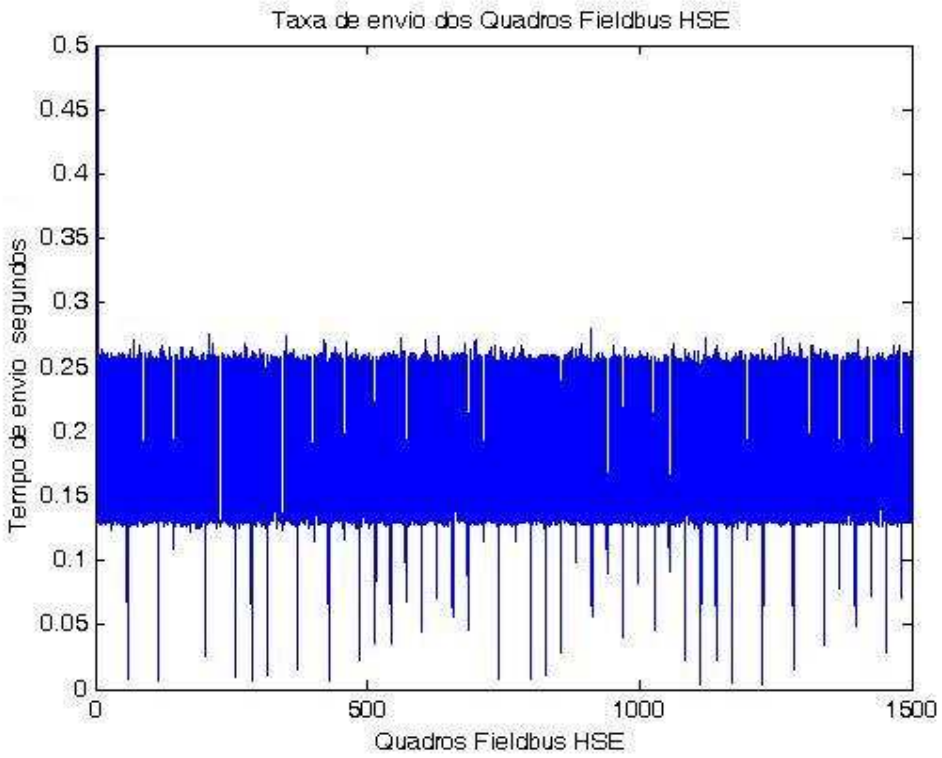


Figura 12. Comportamento padrão HSE

Simultaneamente os quadros analisados na Rede FF-H1 onde funcionam os Reatores Multipropósito dos Casos Estudo I e II obtiveram o intervalo de tempo de envio e recebimento dos quadros padrão FF-H1 de 0,005 a 0,027 segundos, como ilustra a Figura 13, o comportamento dos quadros FF-H1 com o mesmo numero de quadros da amostra na rede LAN.

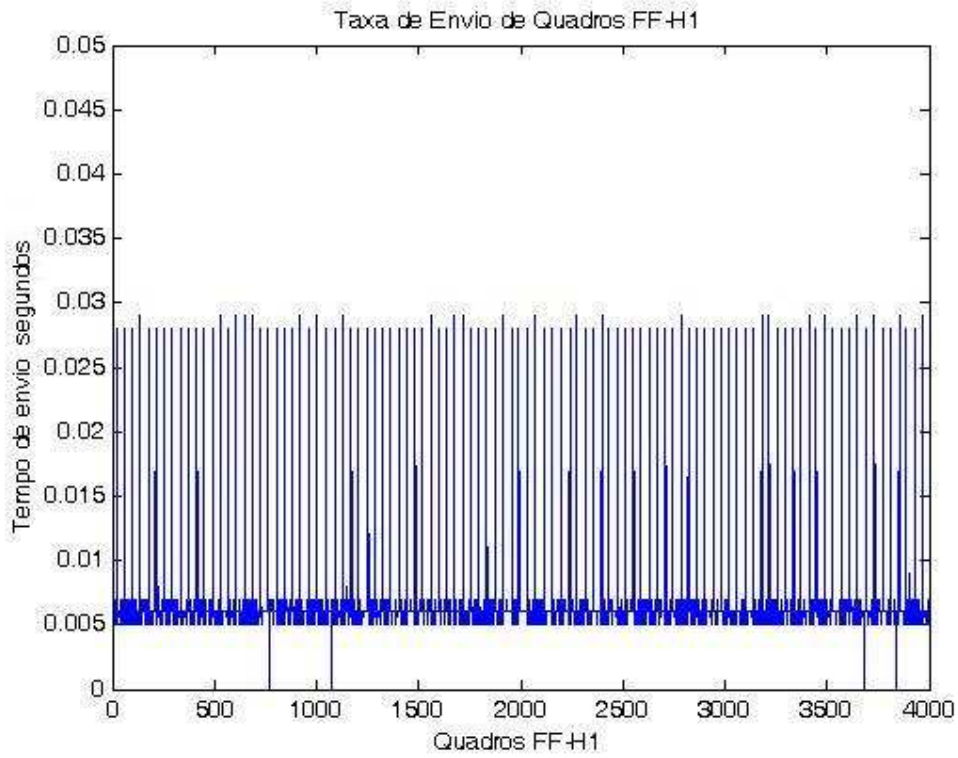


Figura 13. Comportamento da FF-H1.

4.2 Especificação e Instalação.

A malha de aterramento dos Casos-Estudo I e II e a instalação do terminador de rede na FF-H1 no final da rede são mostradas nas imagens da Figura 14.

Com as medidas cabíveis de correção da instalação dos Casos-Estudo I e II levando ao estado normal de funcionamento da rede hibrida (FF-H1, HSE e Ethernet) nos equipamentos; Servidor SCADA I e II, Cliente Local e os DI's, foram observados que não houve problemas de comunicação nos testes do projeto CRAPQ que possam ser caracterizados como ruídos eletromagnéticos, resolvendo definitivamente o problema de instabilidade de comunicação de forma eficaz.

Figura 14. Malha de Aterramento do Caso I e II e Terminador de Rede Fieldbus.

4.2.1 Instalação de equipamentos para comunicação sem fio.

A ausência de dispositivos de rede sem fio inviabilizava que o CRAPQ controlasse o Servidor SCADA III. O Servidor SCADA III que controla o Sistema de Refrigeração está instalado em uma a sala 14 metros de distância do Servidor de Internet e do Servidor SDADA I e II, cuja instalação de cabo par-trançado não existe, portanto sem meio físico de conexão.

Inicialmente foi testado um Roteador de rede sem fio da D'Link® e um ponto de rede via USB do mesmo fabricante. Devido as quatro paredes existentes entre o laboratório que estava instalado o Roteador de rede sem fio e o ponto de rede USB sem fio no laboratório do Servidor SCADA III. Os dispositivos não ofereciam um sinal adequado de radio freqüência suficiente para o enlace da rede. Foi então necessário dimensionar um Roteador de rede de maior potência.

O dispositivo encontrado para suprir um sinal de radio freqüência de maior potência foi o Roteador de rede sem fio da 3Com e o ponto USB foi trocado por placas de rede sem fio do mesmo fabricante, como mostram as imagens da Figura 15.

Figura 15. Roteador 3Com e placa de rede 3Com para rede sem fio.

Resolvidos os dois problemas relacionados ao meio físico que eram a instabilidade da rede hibrida e a ausência de rede sem fio protegida, ficou para ser resolvido o problema da estrutura do Projeto Inicial que apontava um problema gravíssimo no enlace da Rede Virtual Privada entre o Servidor de Internet e o Cliente de Internet, devido à ausência de uma porta exclusiva para a VPN externa do Projeto CRAPQ. Este último obstáculo poderia inviabilizar o projeto como um todo, caso fosse mantida a estrutura original do Projeto Inicial.

Para resolver este problema que o Projeto Inicial indicou, foi mudado toda arquitetura de sistema operacional e de aplicações envolvidas no CRAPQ que foi reestruturado a solucionar este novo problema de forma ágil.

Assim com base na nova estrutura mostrada Tabela 05 e 06 os ensaios de comunicação realizados com base nesta configuração para o CRAPQ foram testadas com sucesso, portanto: os sistemas operacionais, as aplicações, equipamentos e dispositivos, descritos na Tabela 03, que obtiveram resultados de funcionalidade estáveis sob condições normais de funcionamento que são mostrados na Tabela 10.

Tabela 10 - Funcionalidade do projeto final do CRAPQ.

Resultado de Teste Complementar	
Computadores	
Função	**Conclusão de funcionamento**
Servidor de Internet	Estável
Servidor SCADA I e II	Estável
Servidor SCADA III	Estável
Cliente SCADA local I e II	Estável
Cliente SCADA local III	Estável
Cliente de Internet	Estável
Equipamentos	
Função	**Conclusão de funcionamento**
Interface FF-H1 e Ethernet	Estável
Interface de rede local para sem fio	Estável
Interface de rede local	Estável
Sistemas Operacionais	
Função	**Conclusão de funcionamento**
Servidor de Internet	Estável
Servidor SCADA I e II	Estável
Servidor SCADA III	Estável
Cliente SCADA local I e II	Estável
Cliente SCADA local III	Estável
Cliente de Internet	Estável

Tabela 11 - Funcionalidade das aplicações no projeto final do CRAPQ.

Aplicações	
Função	**Resultado de Teste Preliminar**
Servidor de Internet	estável
Servidor SCADA I e II	estável
Servidor SCADA III	estável
Cliente SCADA local I e II	estável
Cliente SCADA local III	estável
Cliente de Internet	estável

Com os resultados apresentados na Tabela 10 e 11 o funcionamento do CRAPQ foi caracterizado na descrição de funcionamento do Projeto Final apresentada no próximo item.

4.3 Descrição do funcionamento do CRAPQ.

Devido o Projeto Inicial ser composto pela arquitetura de sistemas operacionais e aplicações descritas nas Tabelas 03 e 04 e o Projeto Final ser composto pela arquitetura nova descrita nas Tabelas 05 e 06, a descrição do funcionamento do CRAPQ dependeu do teste de funcionalidade do Projeto Final apresentado na seção anterior.

Os experimentos do laboratório estão conectados fisicamente via rede local (LAN). O Servidor de Internet é a interface que faz a ponte (*"Gateway"*) entre a rede local e a rede mundial de computadores e somente através dele podem ser acessados os Servidores SCADA I, II e III. O Servidor de Internet disponibilizou o acesso remoto a todo o sistema por uma VPN criada pela aplicação Logmein®. O Servidor de Internet é Cliente de dois Servidores SCADA cuja configuração foi realizada pelos aplicativos:

- VNC Server® para o Servidor SCADA I, II e III;
- VNC Viewer® para o Cliente SCADA I, II e III.

O Cliente de Internet acessa o Ambiente Virtual (ambiente do Logmein®) por meio de um ou mais usuários e senhas cadastradas no sistema e no Servidor de Internet. O Ambiente Virtual verifica se o Servidor de Internet está ou não ligado no laboratório. Este procedimento é realizado na tela apresentada na Figura 16.

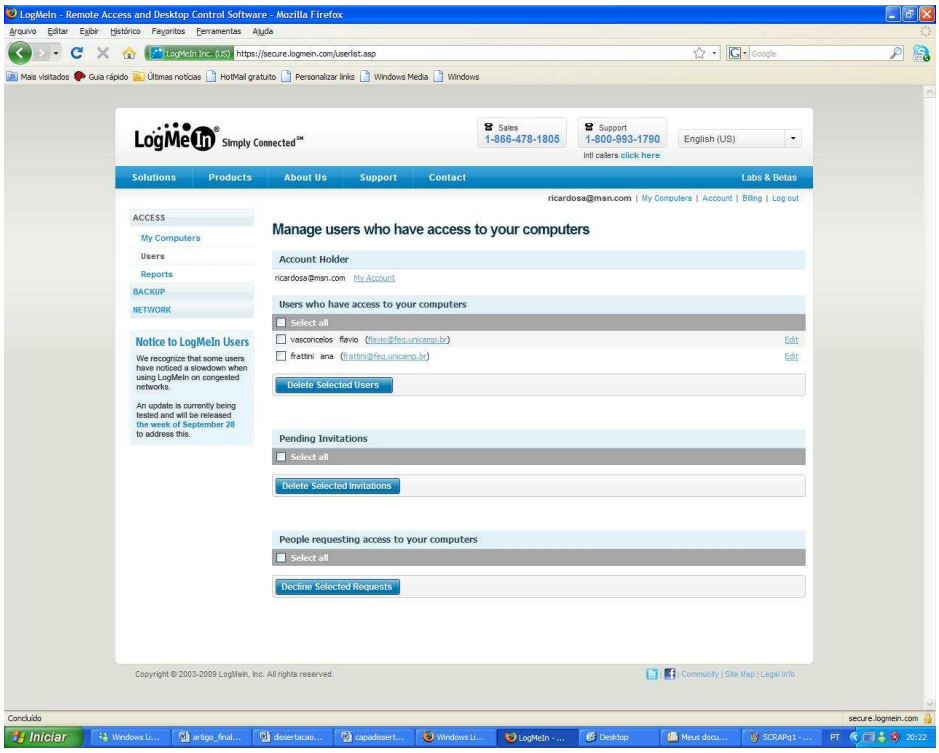


Figura 16. Usuários Cadastrados no Servidor de Internet.

Caso o Servidor de Internet esteja ligado, basta acionar o ícone referente ao Servidor de Internet no Ambiente Virtual e assim estará disponível a tela para a conexão ao Servidor de Internet ilustrado também na Figura 17.

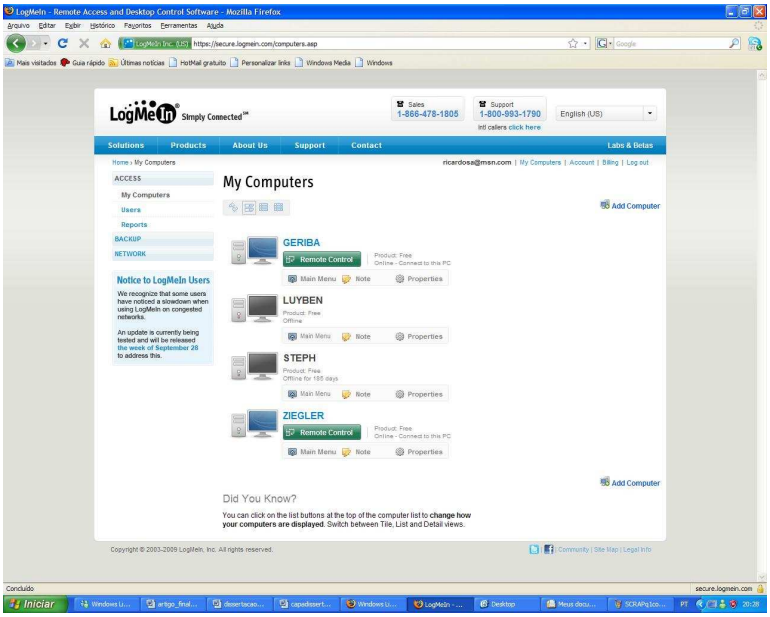


Figura 17. Servidor de Internet Desligado.

O acionamento do ícone no Ambiente Virtual acessou o Servidor de Internet, através do Cliente de Internet, iniciando o processo de conexão ao Servidor de Internet.

Após a conexão, o Ambiente Virtual disponibilizou o acesso remoto ao Servidor de Internet que abriu o acesso aos Servidores SCADA I, II e III. Assim, quando é acionado o ícone de Controle Remoto, mostrado na ilustração da Figura 17, o Cliente de Internet terá acesso ao login do Servidor de Internet, ilustrado na Figura 18.

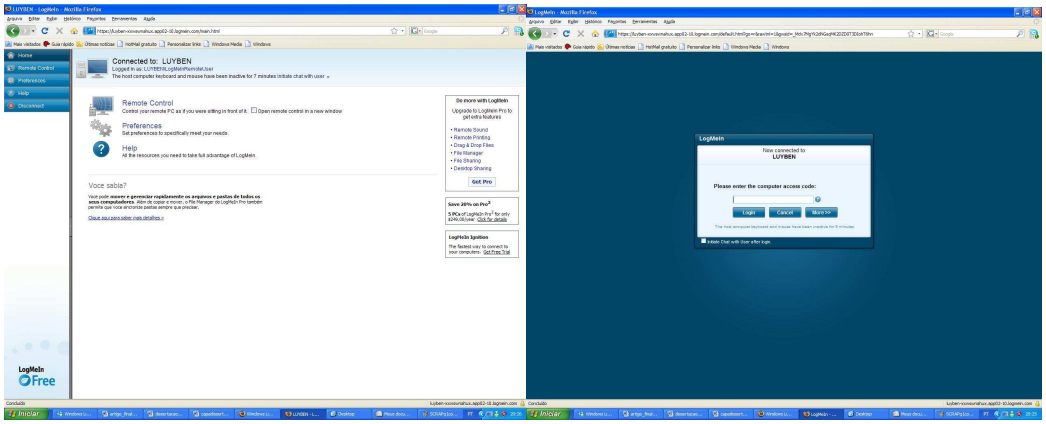


Figura 18. Controle Remoto e requisição de serviço de Acesso ao Servidor de Internet.

A última etapa de acesso ao Servidor de Internet é a Área de escolha de Usuários do Servidor,que é feita assim que a senha do Servidor Local para a disponibilização dos serviços locais é verificada. Neste momento, o Servidor de Internet abre a tela do Sistema Operacional XP® local, como mostra a Figura 19.

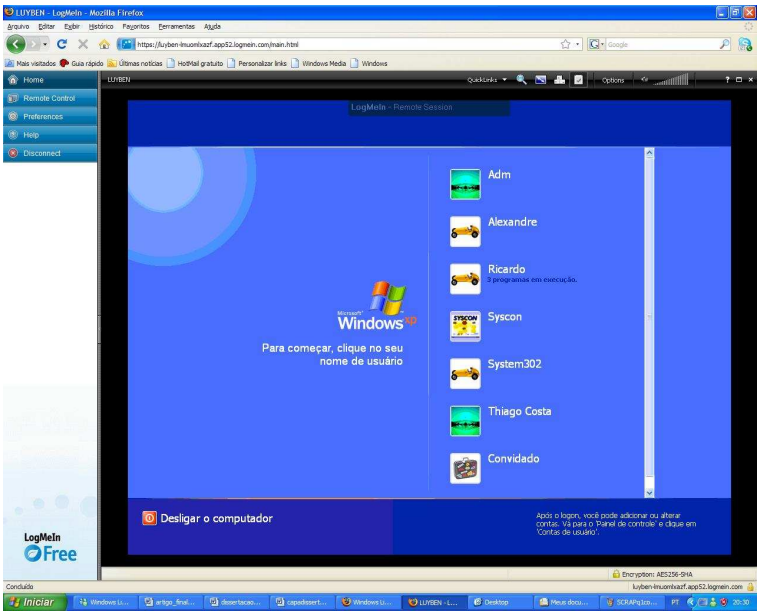


Figura 19. Tela inicial do sistema operacional do Servidor de Internet.

Nas quatro Áreas de Serviço configuradas neste Servidor de Internet, existe um ícone do Cliente VNC Viewer® (Cliente SCADA local) cujo acesso aos Servidores SCADA é realizado pela entrada do endereço de Ponto de Internet (IP) e senha deste Servidor. Ao acionar o ícone do Cliente SCADA local na primeira Área de Serviço são verificados o usuário e a senha pelo sistema de chaves assimétricas do TigthVNC® a 125 bits. Com tais operações a Área de Trabalho do Servidor SCADA é disponibilizada, na Área de Trabalho do Cliente de Internet, que acontecerá após a validação de segurança e o tunelamento serem realizados com sucesso, como mostra a Figura 20.

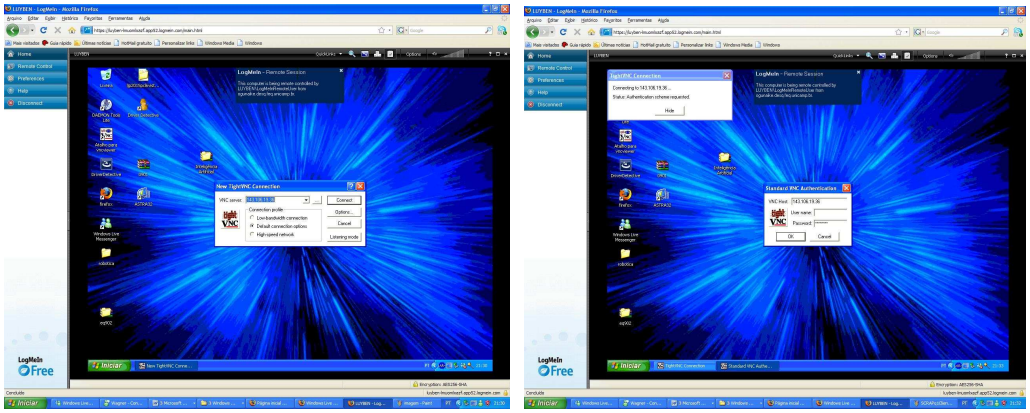


Figura 20. Solicitação do Cliente SCADA I e II.

Com os dois Servidores SCADA acessados em duas Áreas de Serviço diferentes no mesmo Servidor de Internet, como ilustrado na Figura 21, o Cliente de Internet Administra, Supervisiona, Configura e realiza o Controle de Processos nos Reatores Multipropósito e no Sistema de Refrigeração a distância.

Com a configuração do Cliente de Internet, Servidor de Internet, Cliente SCADA local e Servidores SCADA local, os processos no Laboratório de Controle e Automação de Processos (LCAP) são controlados via internet e podem ser operados por meio de qualquer computador, *notebook* ou dispositivo móvel que tenha um navegador de internet compatível ao sistema.

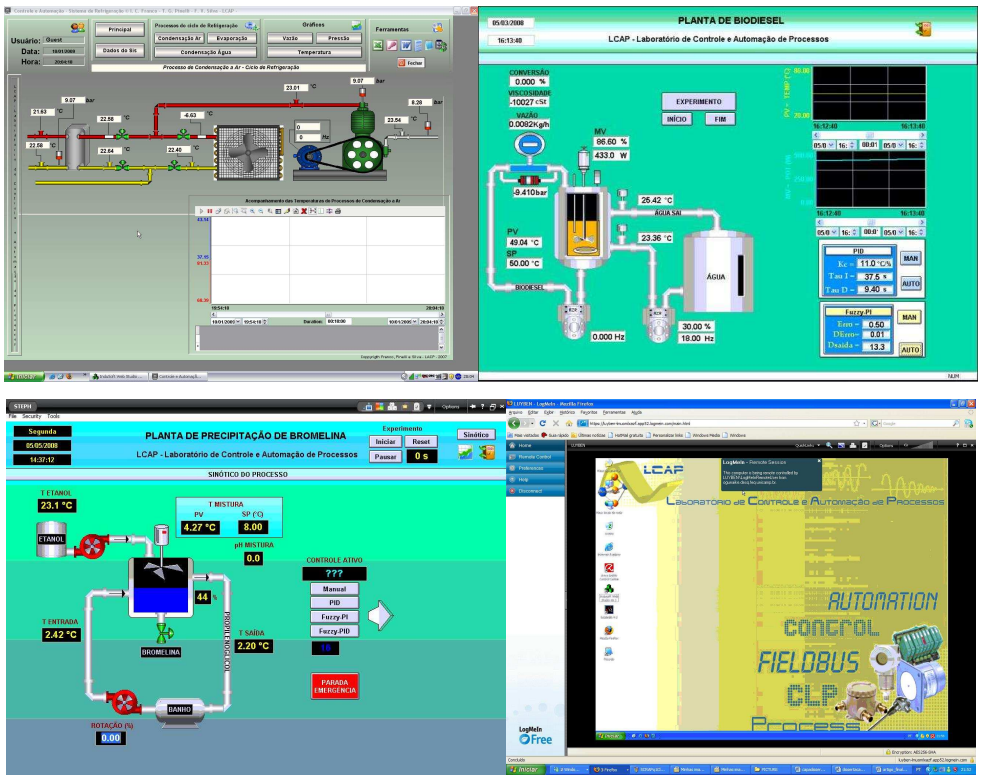


Figura 21. Telas dos Servidores SCADA comutadas pelo Servidor de Internet.

O sistema desenvolvido garante a compatibilidade e a interoperabilidade entre os sistemas de automação diversificados que operam no laboratório. Sendo fácil a configuração de futuros aparatos ao sistema, mantendo a segurança e integridade dos sistemas existentes.

4.4 Resultados dos testes entre Cliente SCADA local I e II e Servidor SCADA I e II

Neste trabalho a primeira Rede Virtual Privada Local (VPN Local) a funcionar foi referente ao Servidor SCADA I e II que disponibiliza o serviço da VPN Local juntamente com os serviços básicos do Sistema Operacional.

A disponibilidade do serviço da VPN Local é criada a partir do aplicativo Cliente Tigth VNC Viewer® (Cliente SCADA I e II), instalado na primeira área de serviço do Servidor de Internet.

O meio físico utilizado foi cabo de par trançado de 6 vias com padrão Ethernet 802.3. O Cliente Local instalado no Servidor de Internet acessa o Servidor SCADA I e II mostrado na imagem da Figura 22.

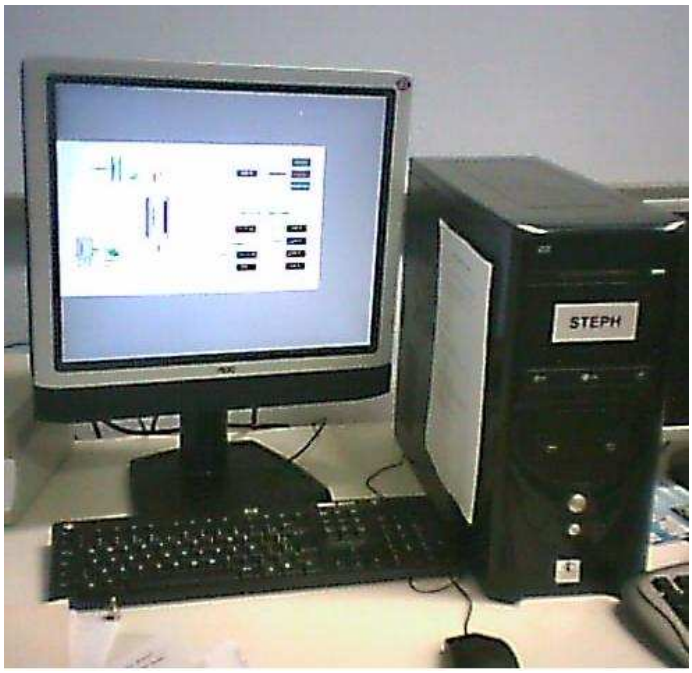


Figura 22. Servidor SCADA I e II

As medidas adquiridas dos testes realizados são apresentadas na Tabela 12, especificando os tempos mínimos, máximos e médios em milisegundos gastos para cada caso dos itens relacionados.

Na última linha da Tabela 12 é mostrada a utilização de rede em percentual relacionado aos demais serviços que são solicitados na mesma rede.

Tabela 12. – Testes entre Cliente SCADA I e II, Servidor SCADA I e II.

Testes de Comunicação			
Descrição	**Tempos em segundos**		
Testes Realizados	Mínimo	Máximo	Média
Tempo de estabelecimento de conexão (TEC I)	0,018402	0,513021	0,380994
Tempo para abrir seção (TAS I)	0,5	2,0	0,8
Tempo de solicitação do mouse (TRD I)	0,008	0,015	0,01
Tempo de solicitação do teclado (TRD I)	0,008	0,015	0,01
Tempo de atualização de vídeo (TAV I)	0,1	0,8	0,3
Tempo de inicialização de programas (TIP I)	2,0	15,0	5,0
Tempo do fechamento de programas	2,0	8,0	5,0
Tempo ao desligar o Servidor SCADA I	11,0	15,0	12,0
Tempo utilizado no fechamento da seção	0,5	2,0	0,7
Utilização da VPN na rede Local em percentual	5%	27%	5%

4.5 Resultados dos Testes entre Cliente SCADA Local III e Servidor SCADA III.

A segunda VPN Local a funcionar refere-se ao Servidor SCADA III. O Servidor SCADA III, da mesma maneira que o Servidor SCADA I e II, disponibiliza o serviço da VPN Local juntamente com os serviços básicos do Sistema Operacional. A disponibilidade do serviço da VPN Local é criada a partir do mesmo aplicativo Cliente Tigth VNC Viewer® (Cliente SCADA III), instalado na segunda área de serviço do Servidor de Internet.

O meio físico utilizado entre o Servidor de Internet e o Servidor SCADA III foi o sinal de radio freqüência aberto pelo roteador de rede sem fio da 3Com padrão Ethernet 802.3.

O Cliente SCADA III, instalado no Servidor de Internet, acessa o Servidor SCADA III, mostrado na Figura 23.

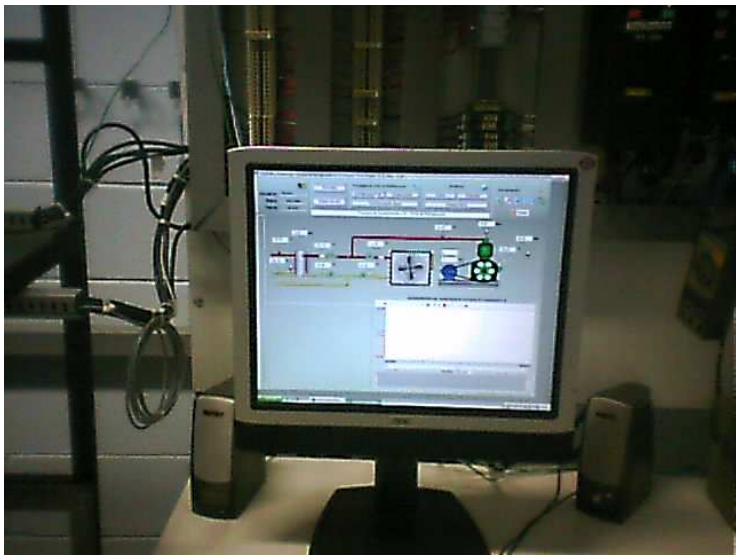


Figura 23. Servidor SCADA III

As medidas adquiridas dos testes realizados são mostradas na Tabela 13 especifi-
cando os tempos mínimos, máximos e médios em segundos gastos para cada caso dos itens relacionados.

Na última linha da Tabela 13 é apresentada a utilização de rede em percentual relacionado aos demais serviços que são solicitados na mesma rede.

Tabela 13. – Testes entre Cliente SCADA III e Servidor SCADA III.

Testes de Comunicação			
Descrição	**Tempos em segundos**		
Testes Realizados	Mínimo	Máximo	Média
Tempo de estabelecimento de conexão (TEC II)	0,21795	1,4875	0,8553
Tempo para abrir seção (TAS II)	0,5	3,0	1,1
Tempo de solicitação do mouse (TRD II)	0,01	0,15	0,09
Tempo de solicitação do teclado (TRD II)	0,01	0,15	0,09
Tempo de atualização de vídeo (TAV II)	0,3	2,5	0,7
Tempo de inicialização de programas (TIP II)	2,0	15,0	5,0
Tempo do fechamento de programas	2,0	8,0	5,0
Tempo ao desligar o Servidor SCADA II	11,0	15,0	12,0
Tempo utilizado no fechamento da seção	0,5	2,0	0,7
Utilização da VPN na rede Local em percentual	7%	30%	9%

4.6 Resultados dos testes entre Cliente de Internet e Servidor de Internet.

A terceira e principal VPN a funcionar foi referente ao Servidor de Internet. O Servidor de Internet disponibiliza o serviço da VPN juntamente com os serviços básicos do Sistema Operacional. A disponibilidade do serviço da VPN na Internet é criada a partir de uma biblioteca de vinculo dinâmico (DLL) instalada no Servidor de Internet pela aplicação LogMeIn®. A aplicação de uso gratuito cria um Ambiente Virtual num Site na internet que informa se o Servidor de Internet está ou não disponível para o acesso remoto ao Cliente de Internet.

O Cliente de Internet deve possuir uma DLL instalada no seu computador, netbook ou notebook. A DLL funciona com os navegadores de internet atuais sendo configurada

pelo próprio usuário no momento de acesso, caso o usuário seja Administrador do equipamento que está sendo configurado naquele momento para o primeiro acesso.

O meio físico utilizado entre o Servidor de Internet e o Cliente de Internet foi par trançado de 6 vias padrão Ethernet 802.1. O Cliente Internet Instalado no equipamento remoto com acesso a internet por quaisquer meio físico estabelece conexão ao Servidor de Internet, mostrado na Figura 24.

Figura 24. Servidor Internet.

O Cliente de Internet é mostrado na imagem da Figura 25 com o Sistema Operacional Windows XP® e o Navegador de Internet Mozilla Firefox® versão 3.0.

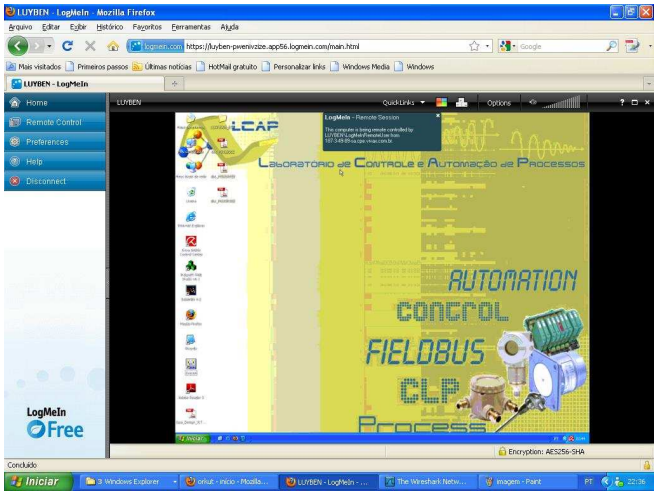


Figura 25. Cliente de Internet remoto e tela do Servidor SCADA I e II.

A Figura 26 mostra a abertura do System302® da SMAR® para configuração de redes Foundation Fieldbus® nos Caso Estudo I e II.

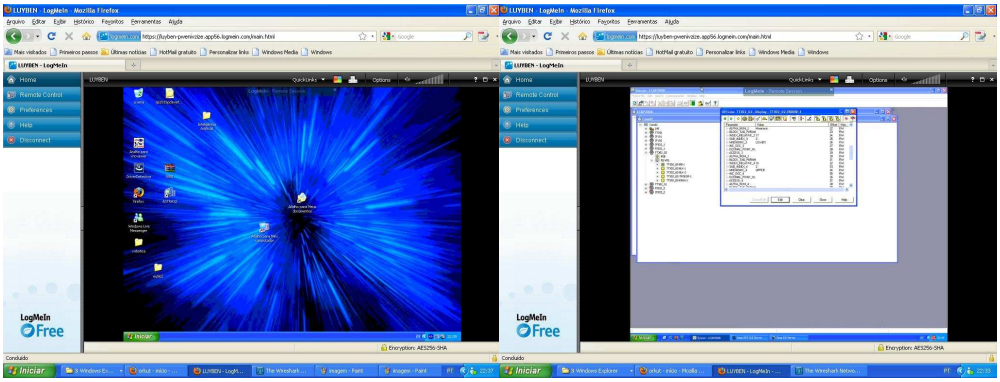


Figura 26 Inicialização de Programas do Servidor SCADA I e II.

A Figura 27 mostra a abertura do Sistema SCADA Indusoft Web Studio® da Indusoft® para desenvolvimento de supervisórios de experimentos no Caso Estudo III.

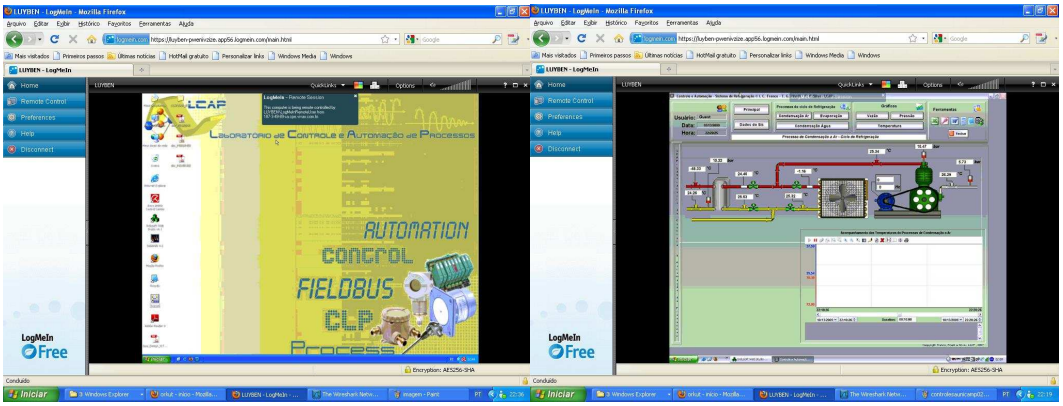


Figura 27 Inicialização de Programas do Servidor SCADA III.

As medidas adquiridas dos testes realizados são mostradas na Tabela 14 especifi-

cando os tempos mínimos, máximos e médios em milisegundos gastos para cada caso dos itens relacionados. Na última linha da Tabela 14 é mostrada a utilização de rede em percentual relacionado demais serviços que são solicitados na mesma rede.

Tabela 14. – Testes entre Cliente de Internet e Servidor de Internet.

Testes de Comunicação			
Descrição	**Tempos em segundos**		
Testes Realizados	Mínimo	Máximo	Média
Tempo de estabelecimento de conexão(TEC IV)	0,304	2,01287	1,4
Tempo para abrir seção (TAV III)	0,892	3,447	1,22
Tempo de solicitação do mouse (TRD III)	0,05	0,5	0,15
Tempo de solicitação do teclado (TRD III)	0,05	0,5	0,15
Tempo de atualização de vídeo (TAV IV)	0,3	3,3	0,8
Tempo de inicialização de programas (TIP IV)	2,0	8,0	5,0
Tempo do fechamento de programas	11,0	15,0	12,0
Tempo ao desligar o Servidor de Internet	13,0	18,0	13,0
Tempo utilizado no fechamento da seção	0,877	3,5	1,15
Utilização da VPN na rede Local em percentual	8%	29 %	12%

4.7 Resultados dos testes de captura de dados transferidos na VPN do sistema CRAPQ.

As informações que trafegam na WAN recebidas ou transferidas do Cliente de Internet são informações sigilosas. Por se tratarem de dados e informações que podem alterar o estado lógico de acionamentos de Máquinas e Processos Químicos industriais, houve uma preocupação excessiva em tornar o sistema robusto e ágil.

A redundância de Criptografia com chaves a 125 bits que é gerada duas vezes pelo sistema dos Servidores SCADA e Servidor de Internet, torna a interpretação de um dado interceptado ilegível a qualquer sistema que utilize uma técnica de rastreamento e captura de dados na internet.

E a decodificação do dado interceptado seria do ponto de vista econômico inviável já que para se quebrar um código por força bruta de 64 bits leva aproximadamente 22 horas e custa cerca de U$250.000,00 por necessitar de um cluster de 1800 processadores (ELETRONIC FRONTIER FOUNDATION).

Segue abaixo a leitura de um dado dentro de um pacote criptografado que foi interceptado na internet durante a operação do Cliente de Internet ao Servidor SCADA III.

O dado interceptado por uma terceira máquina copiou o pacote do protocolo HTTP durante o trafego de informação entre o Cliente de Internet e o Servidor SCADA III, o trafego ocorria num túnel da VPN principal encapsulando outra VPN local pelo algoritmo de segurança do sistema CRAPQ.

“A7AB4C1D3D868509F4504B59CCB2234A61458B6108523B1B...”

O dado criptografado acima representa um acionamento do mouse do Cliente de Internet para a tela de operação do Servidor SCADA III.

Através deste método comprovou-se ser totalmente ilegível e inviável a tentativa computacional de visibilidade do dado enviado ou recebido entre os dois pontos.

5. CONCLUSÕES.

Após o desenvolvimento do CRAPQ os testes realizados através do aplicativo Shark Analizer® demonstraram a velocidade do acionamento dos dispositivos de entrada (mouse e teclado) via conexão remota ao Servidor de Internet a 120 km de distância. O tempo médio do envio do acionamento a partir do Cliente de Internet ao Servidor de Internet foi de 0,195 segundos com uma resposta de atualização de tela média do Servidor de Internet de 1,3 segundos.

As VPN´s entre os Servidores SCADA I e II tiveram um tempo médio de acionamento dos Clientes SCADA I e II de 0,010 e 0,09 segundos, respectivamente, e uma resposta de atualização de tela no Servidor de Internet pelos Clientes SCADA I e II de 0,3 e 0,7 segundos. Concluiu-se então que a soma dos tempos de acionamentos das entradas no Cliente de Internet até o Servidor SCADA I e II foi em média, de 0,151 segundos e o tempo de resposta a este acionamento pela atualização da tela no Cliente de Internet foi em média, 1,1 segundos.

No acionamento das entradas no Cliente de Internet até o Servidor SCADA III o tempo médio foi de 0,24 segundos e o tempo de resposta a este acionamento pela atualização da tela no Cliente de Internet foi em média 1,5 segundos. Assim pode notar-se que a VPN instalada na rede Sem Fio do Servidor SCADA III tem um atraso de 0,089 segundos em relação ao tempo de envio do mesmo acionamento de entrada no Servidor SCADA I e II cujo meio físico é o padrão par trançado. A rede sem fio (radio frequência) apresentou também um atraso no tempo de resposta na atualização da tela do Servidor de Internet de 0,4 segundos.

Em ambas as redes (par trançado e radio frequência) o tempo gasto para o acionamento e resposta de atualização da tela não influenciaram no monitoramento e acionamento remoto dos experimentos no laboratório, principalmente devido o tempo gasto na resposta de correção às perturbações ocorridas experimentos.

Por se tratarem de processos químicos de batelada ou ciclos de refrigeração as mudanças nas variáveis de processo estudadas nestes sistemas, demoram a entrar em regime permanente. Assim as variáveis referentes a taxa de reação ou mudança de temperatura de um ponto de ajuste a outro ocorrem em tempos superiores a 3 minutos para serem monitoradas com exatidão. A variável de resposta mais rápida destes Casos-Estudo foi o acionamento de inversores de freqüência e saídas discretas a válvulas e motores (liga e desliga), estas mudanças de estado corresponderam a uma resposta do sistema de automação de aproximadamente 1,3 segundos, onde o tempo do envio da mensagem de atualização do vídeo foi em média 1,5 segundos gerando assim a visualização do estado da variável no Cliente de Internet.

O desenvolvimento do CRAPQ propiciou o monitoramento, acionamento e controle remoto de Reatores Químicos tipo Multipropósitos e do Equipamento de Refrigeração em tempo real a distâncias extracontinentais pela internet. Onde os experimentos puderam ser acionados, monitorados e administrados independente da tecnologia de automação ou aplicação experimental utilizada, podendo o CRAPQ agregar novos experimentos de forma simples e com funcionamento simultâneo a outros protótipos.

Portanto foi atingido o objetivo principal deste trabalho pela interoperabilidade e facilidade de configuração que o sistema disponibilizou, consequentemente os objetivos secundários foram atingidos através dos resultados obtidos pelos testes descritos na seção 3.

Com a conclusão deste trabalho é plausível afirmar que o acionamento, monitoramento e configuração de diferentes protótipos experimentais aplicados a processos químicos, bioquímicos, e a ciclos de refrigeração, propiciam que laboratórios de pesquisa e centros acadêmicos façam tais operações à distância, em aplicações didáticas e “não criticas” (livre de perigo a pessoas e maquinas).

Os testes realizados nos Caso Estudo I, II e III, através de aplicações de licença livre, abriram uma nova opção ao ensino e pesquisa a distância, pois a utilização de diferentes experimentos em tempo real torna desnecessário que o pesquisador, professor e aluno de graduação esteja no local para realizar as operações acima citadas.

Assim basta o Cliente de Internet ter um dispositivo móvel com o requerimento mínimo e as configurações de segurança ajustadas para que possa interagir com o CRAPQ de qualquer ponto da rede mundial de computadores.

6. SUGESTÕES DE TRABALHOS FUTUROS.

Com os dados obtidos neste trabalho abre novos horizontes de pesquisa nesta área:

- Desenvolvimento de sistemas de segurança remota para plantas químicas.
- Estudo de previsão de estado por RNA para aplicações a distância.
- Gestão da informação em plantas e protótipos químicos, bioquímicos e petroquímicos a distância.
- Projeto de objetos de alarmes para acionamentos de equipamentos e plantas industriais em protocolos abertos.

7. REFERÊNCIAS BIBLIOGRÁFICAS.

1 - AHO, A.V.; HOPCROFT, J.E.; ULLMAN J.D. The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974.

2 - A Norma ANSI/ISA-S50.02-1992, aprovada em 17 de Maio de 1994 -Fieldbus Standard for Use in Industrial Control Systems Part 2: Physical Layer Specification and Service Definition.

3 - ATOS AUTOMAÇÃO INDUSTRIAL LTDA. Micro-Controlador Programável Ref. 3-0055.100 Manual Rev. 1.10 Maio/2004 – Disponível em: <http://www.atos.com.br/download/arquivos/m220011w2p.pdf>.

4 - CLARE W. N.; KAPLAN G. T.; SADLON D. R.; WICTOROWICZ, A. C.; GILBERT, R. A.; WENDT, C. W.; PLC: Programmable Logic Controllers. In: LIPTAK, G. B. Instrument Engineers' Handbook: Process Control and Optimization. 4ª edição. Ed. CRC, Stanford, Connecticut, cap. 5.4, p. 906-908, 2004.

5 - CHENG, T. H. Performance comparison of 100Base-T fast ethernet and 100VG-AnyLAN. Computers & Industrial Engineering, v. 35, cap. 3-4, p. 607-610, 1998.

6 - CORMEN, LEISERSON, RIVEST , CLEIN. Algoritmos: Teoria e prática. Tradução da Segunda edição Americana. Editora Campus, 2002.

7 - COTTLE, J. G. Microprocessors. In: WHITAKER, J. C. The Electronics Handbook Ed. CRC Press, Stamford, Connecticut, cap. 8, p775-784, 2005.

8 - CREEY, A.; BYRES, E. J. Industrial Cybersecurity for power system and SCADA networks. IEEE, Nova York, 2005.

9 - FILETI, A. M. F., PACIANOTTO, T. A., CUNHA, A. P. Neural modeling helps the BOS process to achieve aimed end-point conditions in liquid steel. Engineering Applications of Artificial Intelligence, v. 19, p. 9-17, 2006.

10 - FISHER, D.G. Process control: an overview and personal perspective. (Le controle des operations: une vue d'ensemble et une perspective personnelle). The Canadian Journal Chemical Engenieering, v.69, n.1, p. 5, p. 22, 2009.

11 - GHOSH, S. Distributed Systems: An Algorithmic Approach 2ª edição. Ed. CRC, Stamford, Connecticut, cap. 1, p. 3-10, 2006.

12 - HOROWITZ, E.; SAHNI, S. Fundamentals of Computer Algorithms. Computer Science Press, 1978.

13 - INDUSOFT. Tools for Automation. Produtos: CEView. Disponível em: <http://www.indusoft.com/indusoftart.php?catid=4&name=CEView/CEView/mobile/applications>. Acesso em: 01 mar. 2010.

14 - INDUSOFT. Getting Started. Documen-tation: Indusoft. Disponível em: <http://www.indusoft.com/pdf/Getting_Started_v61.pdf>. Acesso em: 01 mar. 2010.

15 - KOMPELLA K., REKHTER Y. Virtual Private LAN Services Using LDP, Ed. Juniper Networks, 21 Jun. 2006.

16 - KOMPELLA, K.; REKHTER, Y. Virtual Private LAN Service (VPLS) Using BGP for Auto-discovery and Signaling Ed. Juniper Networks, 21 Jun. 2006.

17 - LEITE, M. S., FUJIKI, T. L., SILVA, F. V., FILETI, A. M. F. Determinação de condições operacionais de um processo de precipitação da bromelina via planejamento experimental. In: XVII Congresso Brasileiro de Engenharia Química, Recife, set. 2008.

18 - NATALE, F. Automação Industrial. 2ª edição, Editora Érica, São Paulo, p12-35, 2000.

19 - OTANEZ, P. G.; PARROTT, J. T.; MOUNE, J. R. e TILBURY, D. M. The Implications of Ethernet as a Control Networking Global Powertrain Conference, Ann Arbor, MI, Set. 2002.

20 - ODBC. Disponível em: <http://www.webopedia.com/TERM/O/ODBC.html>. Acesso em: 15 mar. 2010.

21 - OPC Foundation. Disponível em: < http://www.opcfoundation.org /Default.aspx/01_about /01_whatis.asp?MID=AboutOPC >. Acesso em: 10 mar. 2010.

22 - NASA AGENCIA ESPACIAL. Remote Manipulator System. Disponível em: <http://www.nasa.gov/mission_pages/station/structure/elements/jem.html>.Acesso em: 12 de novembro de 2008.

23 - PANTONI, R. P.; BRANDÃO, D. Developing and implementing an open and non-proprietary device description for FOUNDATION Fieldbus based on software stantards. Computers Stantards & Interfaces, Ed. Elsevier, 2009, p. 504-514.

24 - PETERSON, L. L.; DAVIE, B. S. Computer Networks: A Systems Approach 4ª edição. Ed. Morgan Kaufmann, cap2, 116-145, 2007.

25 - PINELLI, T. G. Automação e análise do consumo de energia de um sistema de refrigeração para resfriamento de liquido.Dissertação(Mestrado em Controle de Processos Químicos) – Faculdade de Engenharia Quimica – Unicamp – Campinas, 2008.

26 - RUSSEL, S. e NORVIG, P. Artificial Intelligence – A Modern Approach. Ed. Prentice Hall, New Jersey, p.563 – 597, 1995.

27 - SANTOS, R. L. A. ; SILVA, F. V. ; FILETI, A. M. F. . Adaptive Control of Bromelain Precipitation in Fed-Batch stirred tank. In: International Symposium on Advanced Control of Chemical Process, 2006, Gramado. Proceedings of International Symposium on Advanced Control of Chemical Process. USA : International Federation of Automatic Control, v. II. p. 957-961, 2006.

28 - SANTOS, R. L. A. dos . Controle e monitoramento, em tempo real, de um processo de precipitação de bromelina utilizando comunicação digital fieldbus. Dissertação(Mestrado em Controle de Processos Químicos) - Faculdade Engenharia Quimica – Unicamp, Campinas, 2006.

29 - SILVA, F. V. Comparação do desempenho de um sistema de refrigeração para resfriamento de líquido, controlado a diferentes modos de controle. 2003. 328 f. Tese (Doutorado em Engenharia de Alimentos) 2003 – Faculdade de Engenharia de Alimentos – Unicamp, Campinas, 2003.

30 - SMAR EQUIPAMENTOS INDUSTRIAIS LTDA. Como Implementar projetos com Fieldbus Foundation. Sertãozinho, SP, cap. 2, 51-53 p. Disponível em: <http://www.smar. com/System302/Files/Projetosff/cursofb02.pdf>. Acesso em: 28 jan. 2009.

31 - TANENBAUM, A. S. ; STEEN, M. Distributed Systems: Principles and Paradigms Ed. Prentice Hall, 2002.

32 - TUTHEROW, G. K. Human-Machine Interface Evolution. In: LIPTAK, G. B. Instrument Engineers' Handbook: Process Control and Optimization. 4ª edição. Ed. CRC, Stanford, Connecticut, cap. 4.17 p. 790-804, 2005.

33 - VITTURI, S. System Integration: Computers with PLC. In: LIPTAK, G. B. Instrument Engineers' Handbook: Process Control and Optimization. 4ª edição. Ed. CRC, Stamford, Connecticut, cap. 5.11, p. 1023-1025, 2005.

34 - SHARPE, R. Wireshark - User's Guide <http://www.wireshark.org /docs/wsug_html_chunked/>. Acesso em: 01 mar. 2010.

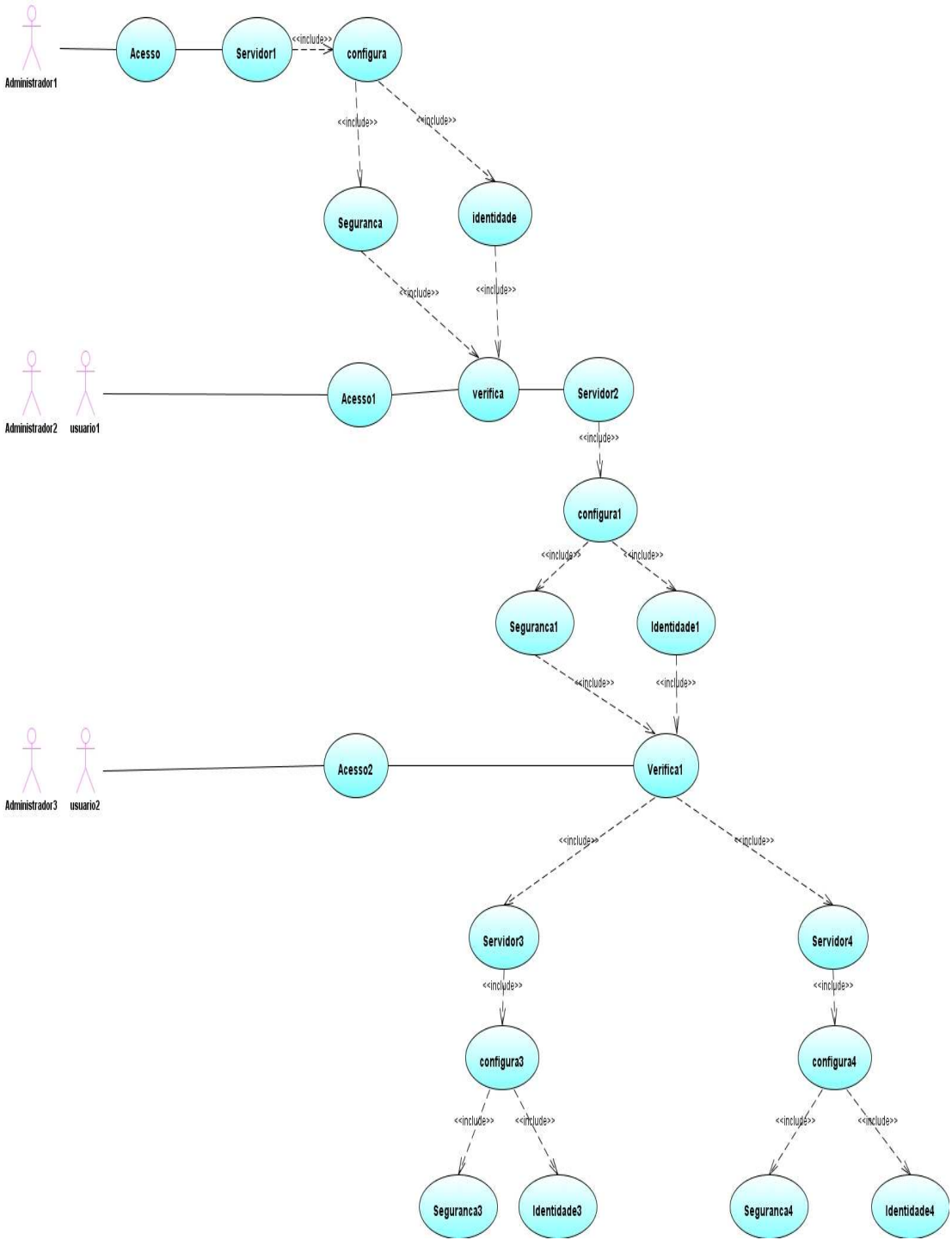
35 - SOCORICELLI, J. M., Juniper Networks Certified Internet Specialist Study Guide, Ed. Sybex , 1ª edição. 2004.

36 - ZIELINSK, M. Digital fieldbus istallations use EDDL for simplicity with advanced, full functionality, Computing and Control Engenieering Journal. London, v.15, p. 24-31, 2005.

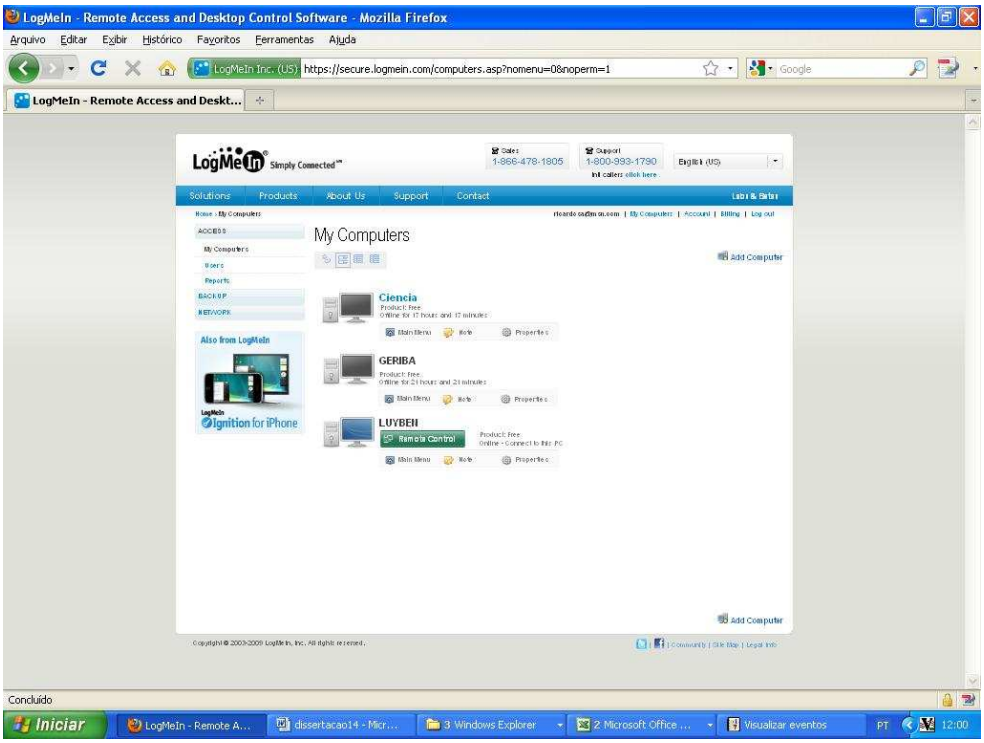
37 - ELETRONIC FRONTIER FOUNDATION, Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design <http://www.ic.unicamp.br/~lucchesi/cracking-des/cracking-des.htm>. Acessado 8 abr. 2010.

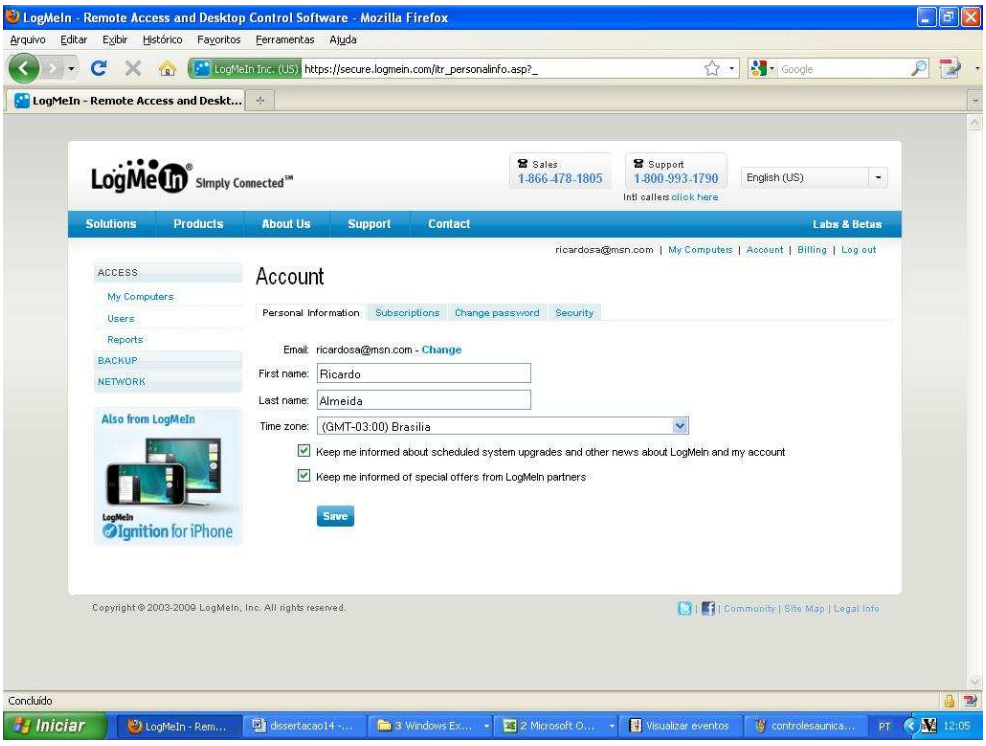
38 - UML - UNIFIED MODELING LANGUAGE. <http://www.uml.org/>. Acessado: 8 abr. 2010.

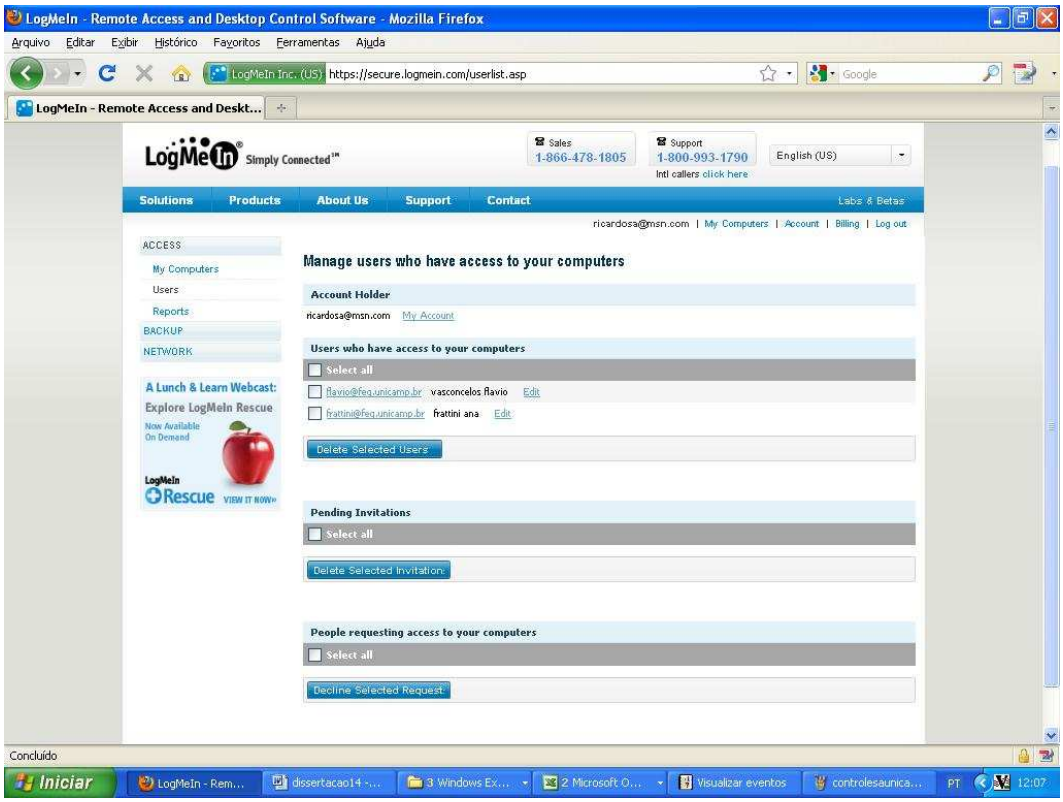
8. APENDICE – I


Administrador1
Acesso
Servidor1
<<include>>
configura
<<include>>
<<include>>
Seguranca
identidade
<<include>>
<<include>>
Administrador2
usuario1
Acesso1
verifica
Servidor2
<<include>>
configura1
<<include>>
<<include>>
Seguranca1
Identidade1
<<include>>
<<include>>
Administrador3
usuario2
Acesso2
Verifica1
<<include>>
<<include>>
Servidor3
Servidor4
<<include>>
<<include>>
configura3
configura4
<<include>>
<<include>>
<<include>>
<<include>>
Seguranca3
Identidade3
Seguranca4
Identidade4

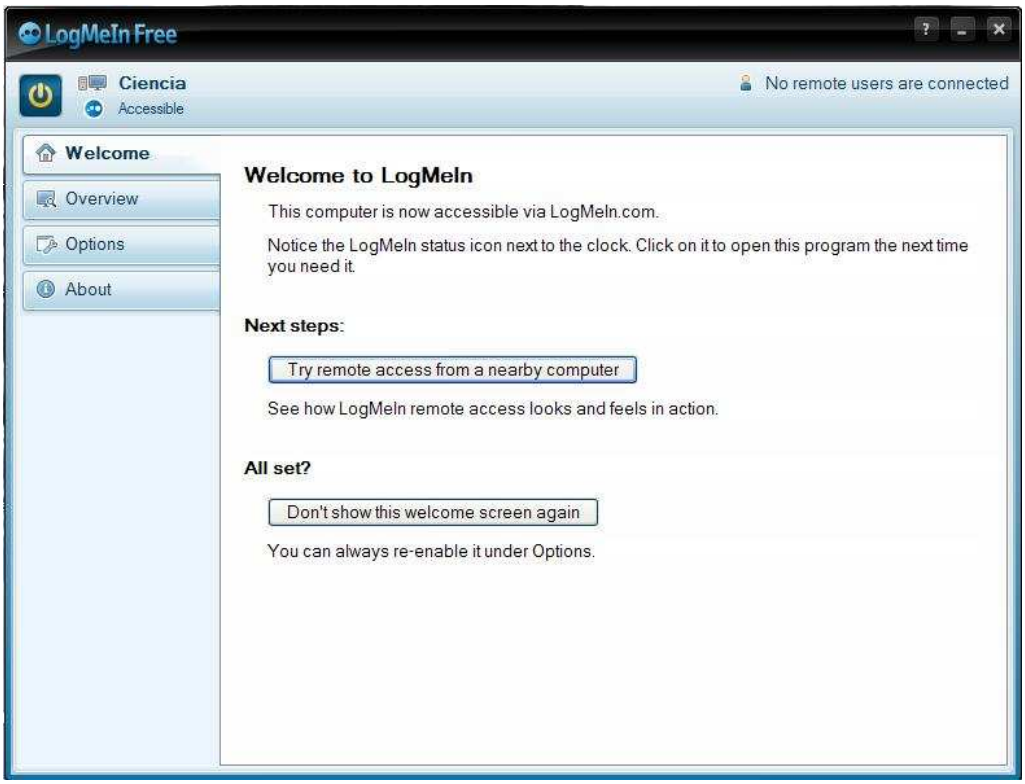
9. APENDICE – II

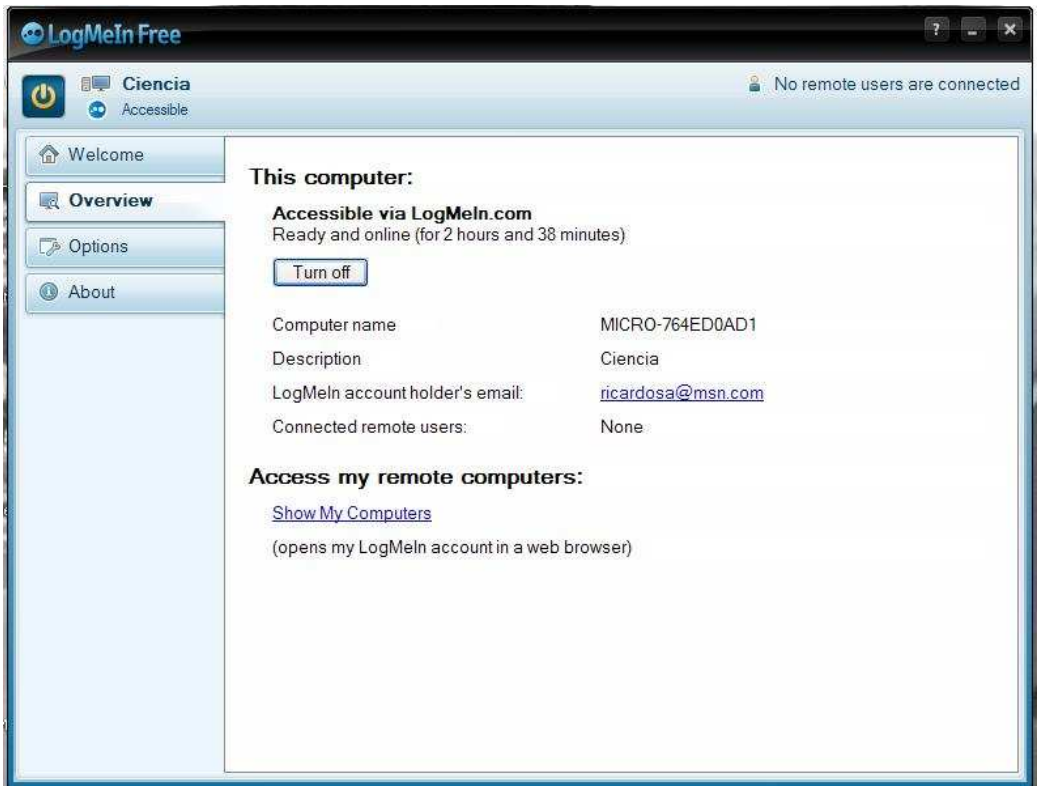




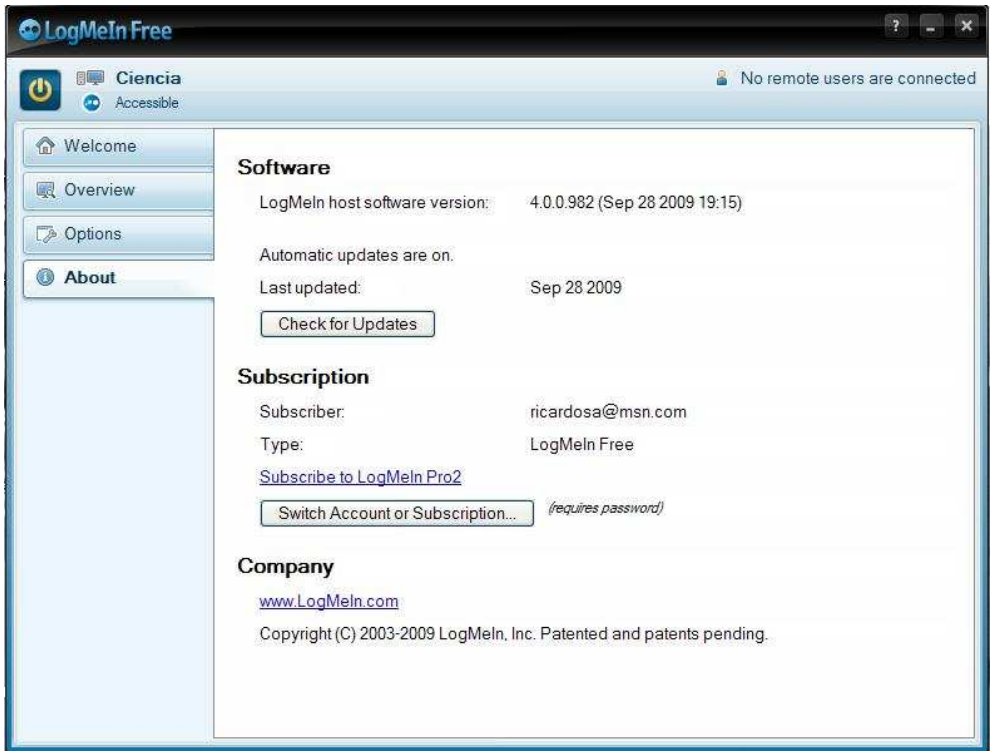

LogMeIn - Remote Access and Desktop Control Software - Mozilla Firefox
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
https://secure.logmein.com/userlist.asp
LogMeIn - Remote Access and Deskt...
Simply Connected
Sales 1-866-478-1805
Support 1-800-993-1790
Intl callers click here
English (US)
Solutions Products About Us Support Contact Labs & Betas
ricardosa@msn.com | My Computers | Account | Billing | Log out
ACCESS
My Computers
Users
Reports
BACKUP
NETWORK
A Lunch & Learn Webcast:
Explore LogMeIn Rescue
Now Available On Demand
LogMeIn Rescue VIEW IT NOW»
Manage users who have access to your computers
Account Holder
ricardosa@msn.com My Account
Users who have access to your computers
Select all
flavio@feq.unicamp.br vasconcelos flavio Edit
frattini@feq.unicamp.br frattini ana Edit
Delete Selected Users
Pending Invitations
Select all
Delete Selected Invitation
People requesting access to your computers
Select all
Decline Selected Request
Concluído
Iniciar
LogMeIn - Rem...
dissertacao14 -...
3 Windows Ex...
2 Microsoft O...
Visualizar eventos
controlesaunica...
PT
12:07

10. APENDICE – III

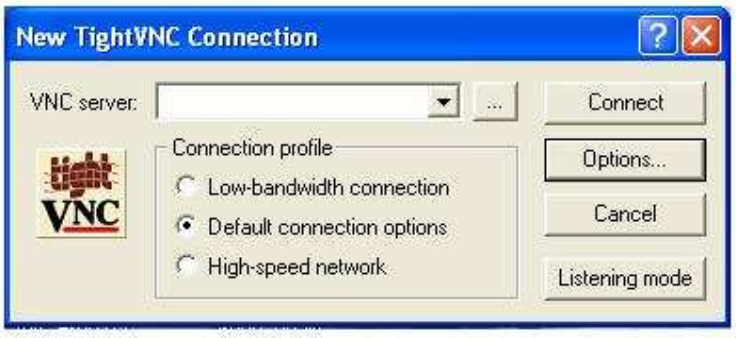


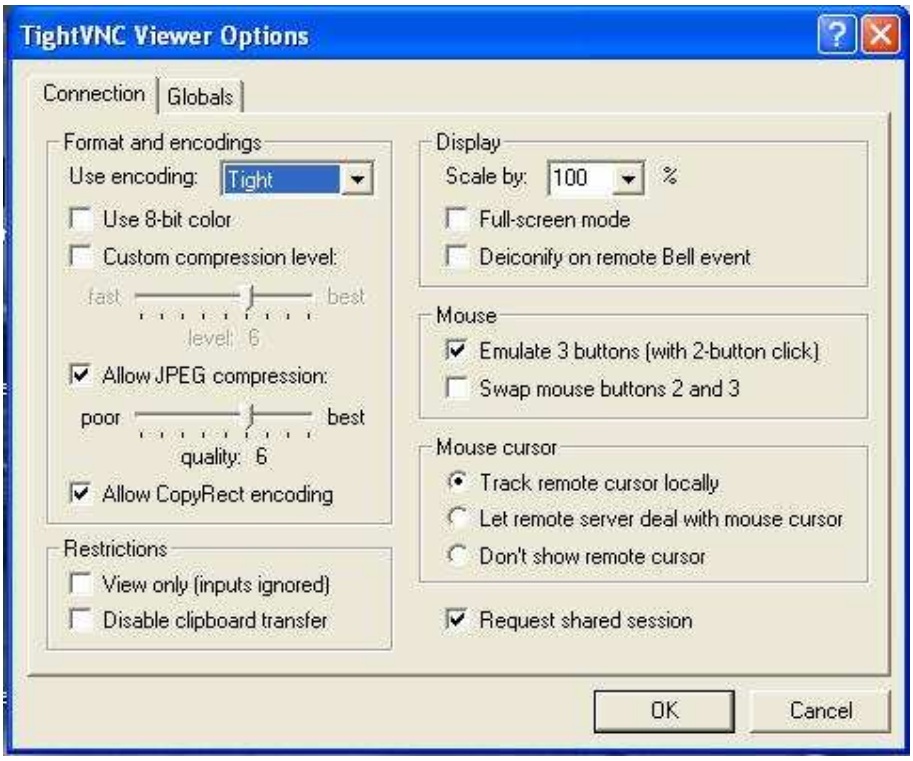


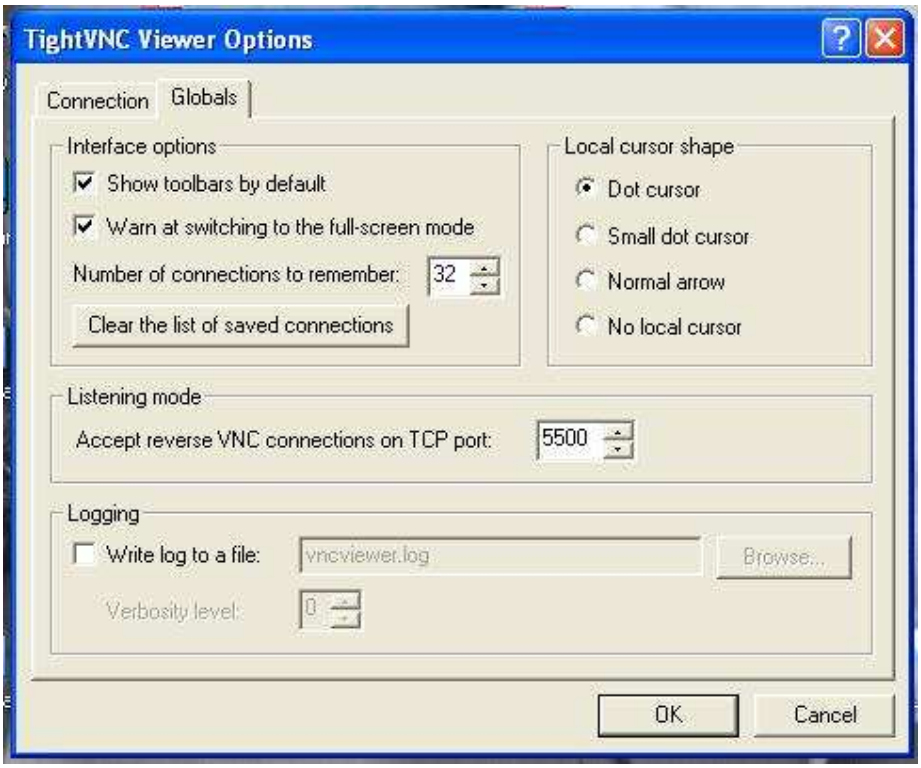

LogMeIn Free
Ciencia
Accessible
No remote users are connected
Welcome
Overview
Options
About
Password
This computer is set up to not require a Windows password at system startup.
To protect the computer from unauthorized access, remote users will need to enter a Computer Access Code.
Change Computer Access Code...
Preferences and Security
Configure how LogMeIn works on this computer.
Preferences
Connection and Event Monitor
View technical information about the LogMeIn software on this computer.
Connection and Event Details
Welcome Screen
Display the Welcome screen when LogMeIn is started.


LogMeIn Free
Ciencia
Accessible
No remote users are connected
Welcome
Overview
Options
About
Software
LogMeIn host software version: 4.0.0.982 (Sep 28 2009 19:15)
Automatic updates are on.
Last updated: Sep 28 2009
Check for Updates
Subscription
Subscriber: ricardosa@msn.com
Type: LogMeIn Free
Subscribe to LogMeIn Pro2
Switch Account or Subscription...
(requires password)
Company
www.LogMeIn.com
Copyright (C) 2003-2009 LogMeIn, Inc. Patented and patents pending.

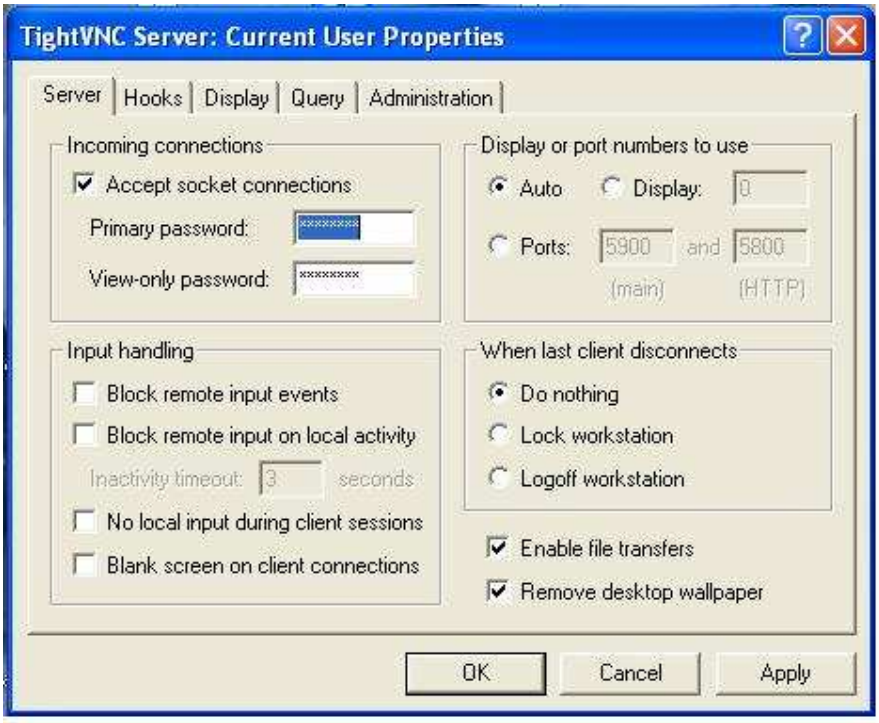
11. APENDICE IV

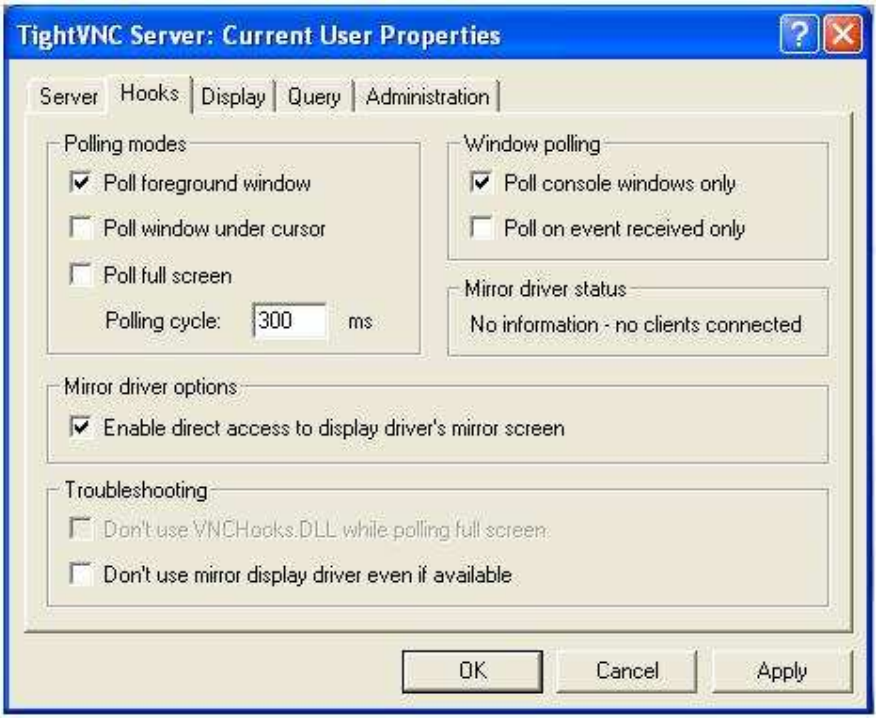


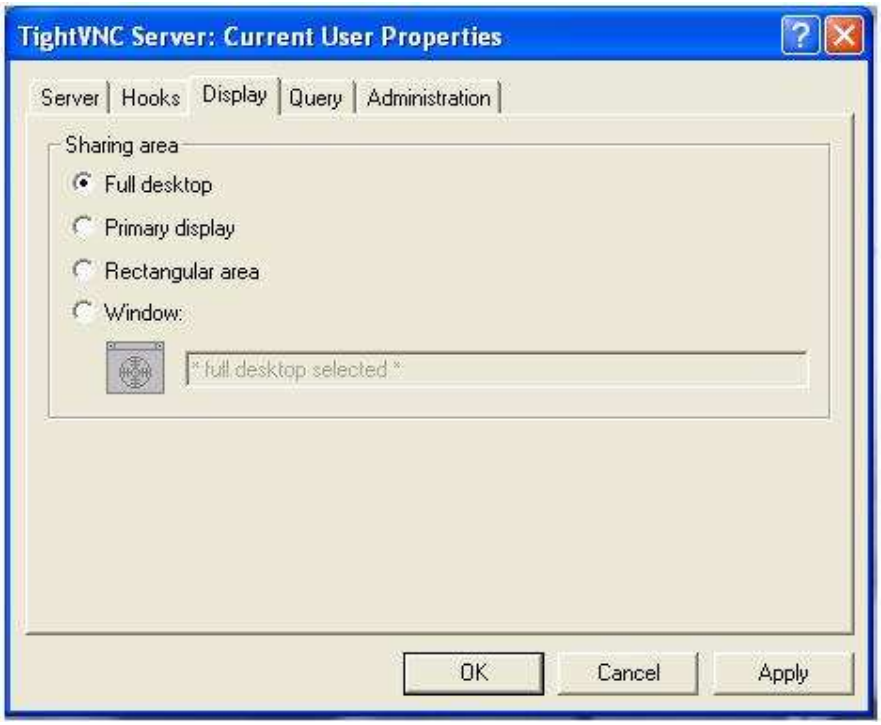


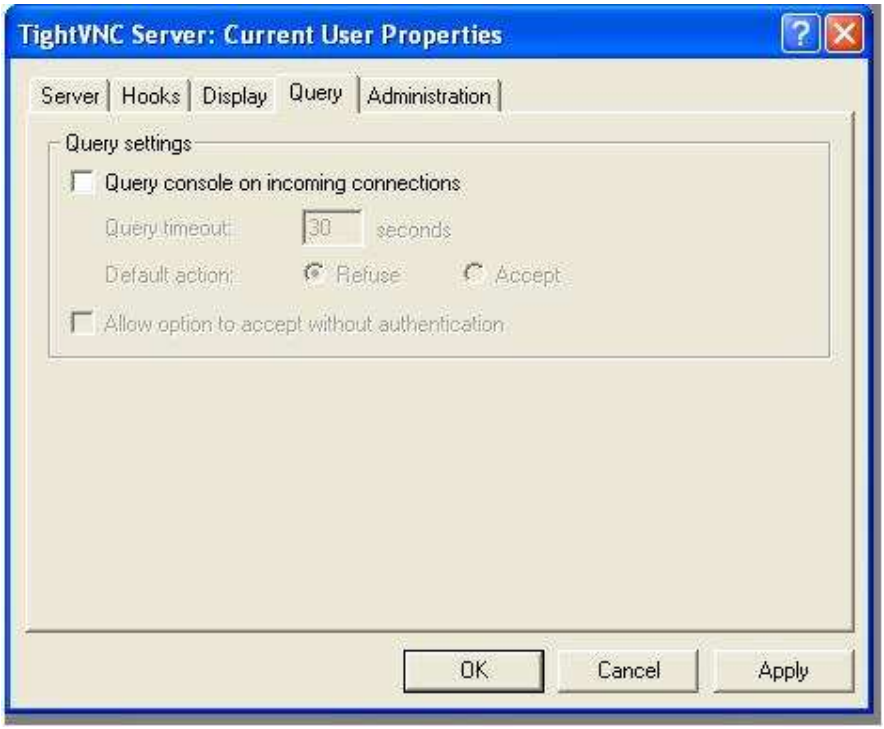

TightVNC Viewer Options
Connection
Globals
Interface options
Show toolbars by default
Warn at switching to the full-screen mode
Number of connections to remember:
32
Clear the list of saved connections
Local cursor shape
Dot cursor
Small dot cursor
Normal arrow
No local cursor
Listening mode
Accept reverse VNC connections on TCP port:
5500
Logging
Write log to a file:
vncviewer.log
Browse...
Verbosity level:
0
OK
Cancel

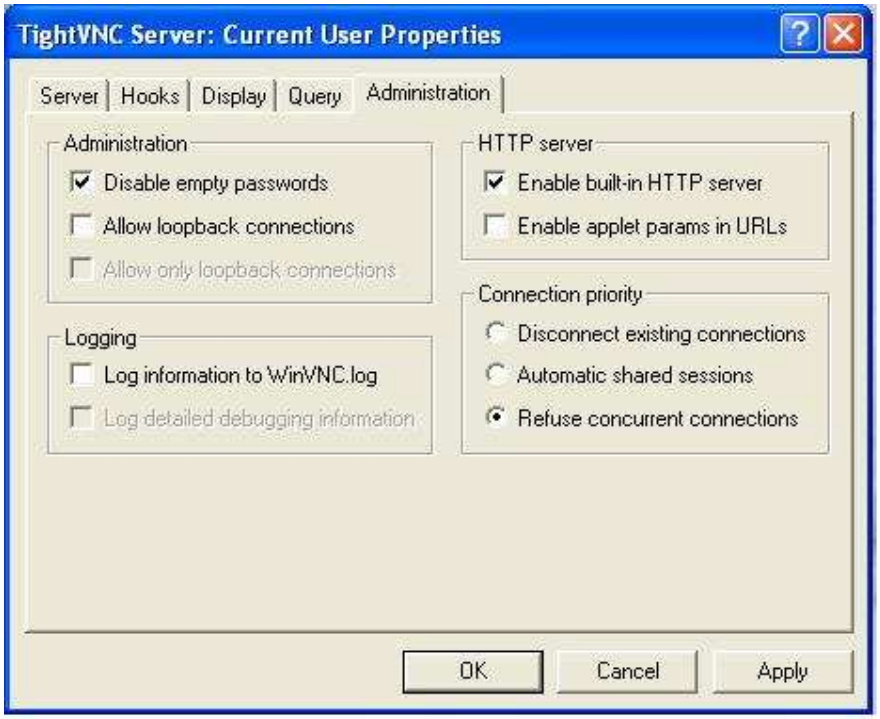
12. APENDICE V



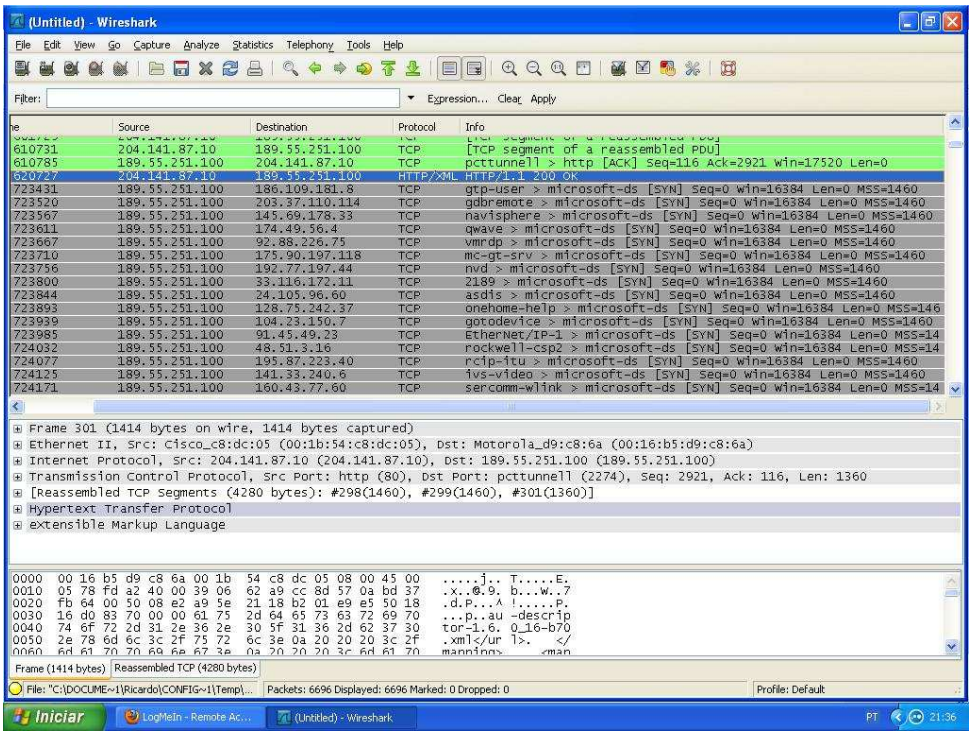


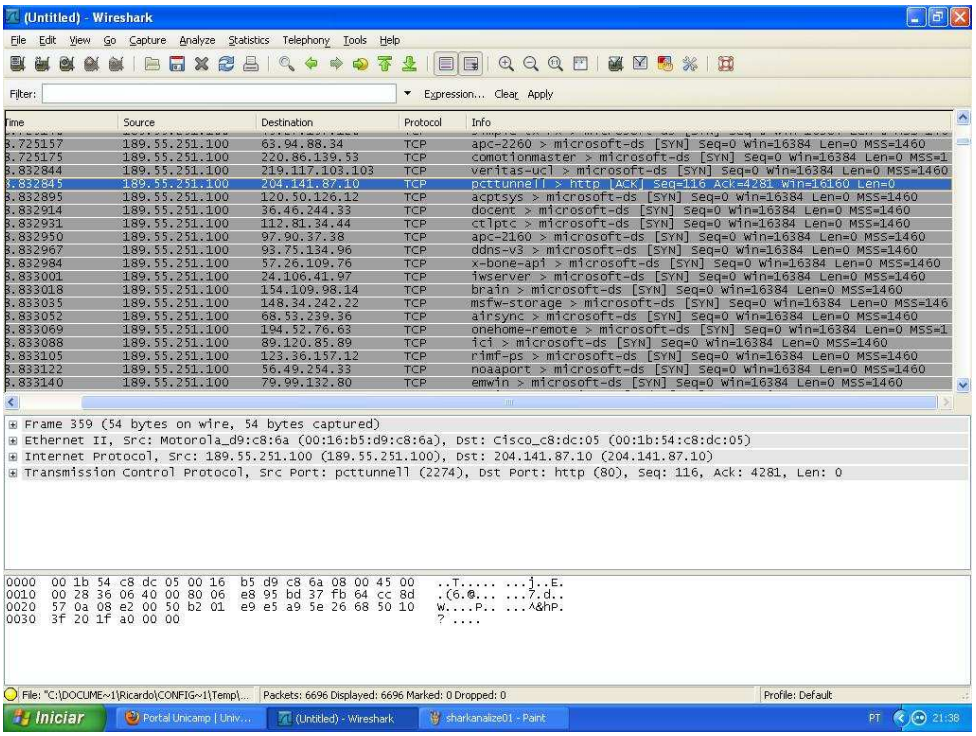

TightVNC Server: Current User Properties
Server
Hooks
Display
Query
Administration
Sharing area
Full desktop
Primary display
Rectangular area
Window:
* full desktop selected *
OK
Cancel
Apply

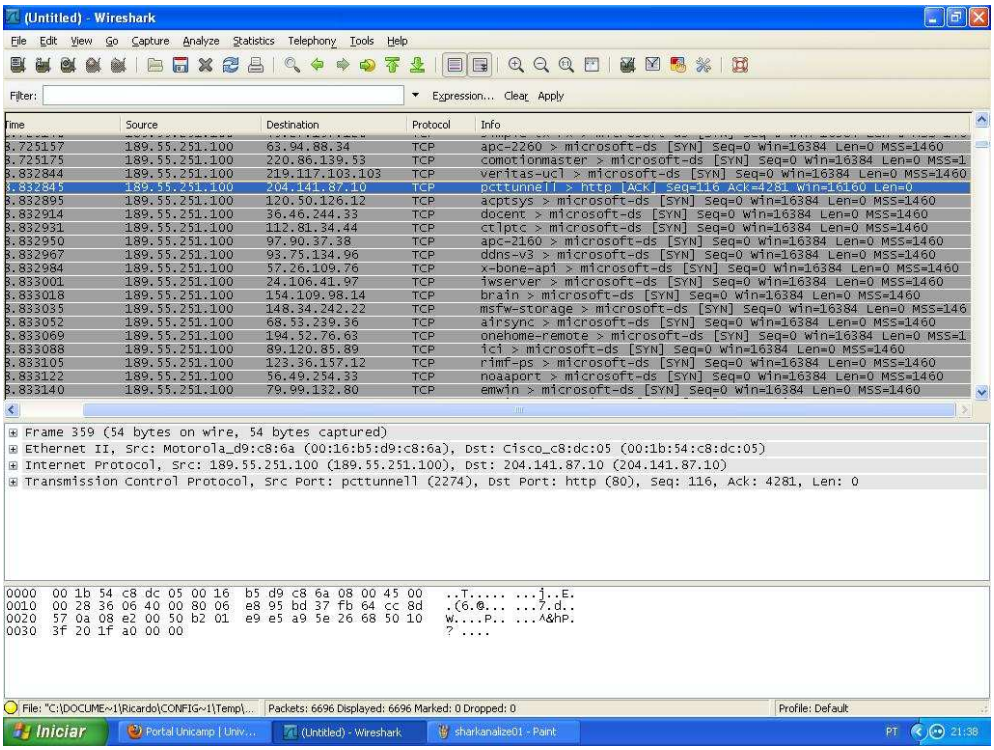

TightVNC Server: Current User Properties
Server
Hooks
Display
Query
Administration
Query settings
Query console on incoming connections
Query timeout:
30
seconds
Default action:
Refuse
Accept
Allow option to accept without authentication
OK
Cancel
Apply


TightVNC Server: Current User Properties
Server
Hooks
Display
Query
Administration
Administration
Disable empty passwords
Allow loopback connections
Allow only loopback connections
Logging
Log information to WinVNC.log
Log detailed debugging information
HTTP server
Enable built-in HTTP server
Enable applet params in URLs
Connection priority
Disconnect existing connections
Automatic shared sessions
Refuse concurrent connections
OK
Cancel
Apply

13. APENDICE - VI






(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
Time Source Destination Protocol Info
3.725157 189.55.251.100 63.94.88.34 TCP apc-2260 > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.725175 189.55.251.100 220.86.139.53 TCP comotionmaster > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1
3.832844 189.55.251.100 219.117.103.103 TCP veritas-ucl > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832845 189.55.251.100 204.141.87.10 TCP pcttunnell > http [ACK] Seq=116 Ack=4281 Win=16160 Len=0
3.832895 189.55.251.100 120.50.126.12 TCP acptsys > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832914 189.55.251.100 36.46.244.33 TCP docent > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832931 189.55.251.100 112.81.34.44 TCP ctlptc > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832950 189.55.251.100 97.90.37.38 TCP apc-2160 > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832967 189.55.251.100 93.75.134.96 TCP ddns-v3 > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.832984 189.55.251.100 57.26.109.76 TCP x-bone-api > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833001 189.55.251.100 24.106.41.97 TCP iwserver > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833018 189.55.251.100 154.109.98.14 TCP brain > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833035 189.55.251.100 148.34.242.22 TCP msfw-storage > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=146
3.833052 189.55.251.100 68.53.239.36 TCP airsync > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833069 189.55.251.100 194.52.76.63 TCP onehome-remote > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1
3.833088 189.55.251.100 89.120.85.89 TCP ici > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833105 189.55.251.100 123.36.157.12 TCP rimf-ps > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833122 189.55.251.100 56.49.254.33 TCP noaaport > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3.833140 189.55.251.100 79.99.132.80 TCP emwin > microsoft-ds [SYN] Seq=0 Win=16384 Len=0 MSS=1460
Frame 359 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: Motorola_d9:c8:6a (00:16:b5:d9:c8:6a), Dst: Cisco_c8:dc:05 (00:1b:54:c8:dc:05)
Internet Protocol, Src: 189.55.251.100 (189.55.251.100), Dst: 204.141.87.10 (204.141.87.10)
Transmission Control Protocol, Src Port: pcttunnell (2274), Dst Port: http (80), Seq: 116, Ack: 4281, Len: 0
0000 00 1b 54 c8 dc 05 00 16 b5 d9 c8 6a 08 00 45 00 ..T..... ...j..E.
0010 00 28 36 06 40 00 80 06 e8 95 bd 37 fb 64 cc 8d .(6.@... ...7.d..
0020 57 0a 08 e2 00 50 b2 01 e9 e5 a9 5e 26 68 50 10 W....P.. ...^&hP.
0030 3f 20 1f a0 00 00 ? ....
File: "C:\DOCUME~1\Ricardo\CONFIG~1\Temp\... Packets: 6696 Displayed: 6696 Marked: 0 Dropped: 0 Profile: Default
Iniciar
Portal Unicamp | Univ...
(Untitled) - Wireshark
sharkanalize01 - Paint
PT
21:38

14. GLOSSÁRIO

ASI – Rede de comunicação industrial baseada no conceito fieldbus.

Browser – ou Navegadores de internet, programas que interpretam HTML.

Bytecodes - É um código binário para uma máquina virtual Java.

CISC - Complex Instruction Set Computer, Computador com um Conjunto Complexo de Instruções é uma arquitetura de processadores capaz de executar centenas de instruções complexas compatível com a Intel e x386 padrão PC.

CORBA – Common Object Request Broker Architecture. É uma arquitetura padrão criada para estabelecer e simplificar a troca de dados entre sistemas distribuídos heterogêneos **Criptografia Assimétrica -** A criptografia assimétrica usa um par de chaves pública/privada. Onde os dados são criptografados com a chave publica e somente podem ser descriptografados por chaves privadas.

Dial –up – Padrão de conexão discada via MODEN

ERP - Enterprise Resource Planning ou Sistemas Integrados de Gestão Empresarial são sistemas de informações que integram todos os dados e processos de uma organização em um único sistema (Laudon[1], Padoveze[2]).

Ethernet IEEE 802.3 – Padrão de conexão via cabo de rede.

Fieldbus Foundation - Rede de comunicação industrial baseada na rede Hart onde o sinal de comunicação é modulado na alimentação do instrumento de campo.

FIREWALL – È um software que bloqueia portas indesejadas que acessam um computador ou uma rede.**Freeware -** Programa de computador cuja utilização não implica no pagamento de licenças de uso ou "**royalties"**. Apesar de ser chamado de "***free"*** (do inglês *livre*), este software não é necessariamente software livre, pode não ter código aberto e pode acompanhar licenças restritivas, limitando o uso comercial, a redistribuição não autorizada, a modificação não autorizada ou outros tipos de restrições.

Flash – Memória Baseados na tecnologia “Flash”, criada no Japão pela Toshiba em 1984, os cartões são memórias do tipo não volátil, as memórias flash têm como principal característica permitir a gravação e leitura de dados aleatoriamente, sem que seja preciso respeitar uma ordem prévia.Permitem acessar mais rapidamente informações e com baixo consumo de energia.

Gateway - Porta de ligação, é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

Hart – Antiga rede de comunicação industrial muito utilizado na indústria quimica e petroquímica.

IHM – Interface homem maquina.

Interbus – Rede de comunicação industrial baseada no conceito de Fieldbus muito utilizada na automação de equipamentos realizam deslocamento de objetos e tratam sinais de velocidade.

JAVA™ - Plataforma de programação da SUN Micro systems que executa programas através de uma maquina virtual interpretado pelo navegador de internet.

JRE – Java Runtime Environment Livraria de atualização para compatibilidade de novas tecnologias.

LAN - LAN - Local Area Network é uma rede de computadores local.

MAN* - MEtropolitan Area NEtwork é uma rede metropolitana de computadores que interliga mais de uma cidade.

Multiplataforma – Diversidade de Sistemas Operacionais

.NET – É uma plataforma de desenvolvimento criada pela Microsoft orientada à criação de software para Internet.

Open Source – Softwares que possuem registro de propriedade intelectual mas possuem o Código Fonte Aberto para sugestões e participação de desenvolvedores no projeto.

PHP - Hypertext Preprocessor é uma linguagem de script open source de uso geral, muito utilizada e especialmente guarnecida para o desenvolvimento de aplicações Web embútivel dentro do HTML.

PID – Função de controle Proporcional Integral e Derivada

PLC - Controlador Lógico Programável hardware desenvolvido para suprir as freqüentes modificações de lógica e comandos eletroeletrônicos na indústria automotiva.

Profbus – Rede de comunicação baseada no conceito fieldbus porem utilizam unidades de processamento de sinais remotas.

Protocolos Dedicado – são padrões de comunicação que são de caráter particular, e possui registro de patente industrial.

Protocolo IPX - É um protocolo nativo do Netware sistema operacional cliente-servidor da Novell.

SCADA – Supervisório de Controle e Aquisição de Dados

SDCD - O Sistema Digital de Controle Distribuído

Servidor APACHE – O Apache é um servidor de paginas de internet que funciona em diversos sistemas operacionais.

Sistemas Operacionais – Os O.S. podem ser considerados gerenciadores e manipuladores de dispositivos, arquivos e tarefas de agendamento e de computação. Alem de servirem de Interface entre os dispositivos, softwares e o homem.

Smartfone – Aparelho de transmissão de voz,dados que reune a funcionalidade de um PC em um telefone celular.

SOAP - O Simple Object Access Protocol é um protocolo elaborado para facilitar a chamada remota de funções via Internet, permitindo que dois programas se comuniquem de uma maneira tecnicamente muito semelhante à invocação de páginas Web.

SSH - "**Secure shell"**, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota. Possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.

Supervisório – Software que faz a supervisão de sistemas de automação industriais.

TELNET - Protocolo de Terminal Virtual é um protocolo de Internet para estabelecer a conexão entre computadores. Através dessa conexão remota, pode-se executar programas e comandos em outra máquina, como se o teclado de seu computador estivesse ligado diretamente a ela.

TCP/IP – **"Transfer control protocol",** Protocolo de controle e transporte **/** "**Identify protocol",** Protocolo de identificação.

VBScript - Visual Basic Script Language é uma linguagem de programação desenvolvida para rodar aplicações no servidor remoto.

Virtual Machines - Um programa em Java é compilado para o chamado "byte-code", que é próximo às instruções de máquina, mas não de uma máquina real.

VPN – "**Virtual Private Network",** Rede privada virtual.

WAN - World Area Network é a rede mundial de computadores Internet.

Wireless IEEE 802.11 – Padrão de conexão sem fio via radio freqüência.