Departamento de Engenharia Electrotécnica

# MONITORIZAÇÃO INTEGRADA PARA SISTEMAS DE ALIMENTAÇÃO DISTRIBUÍDOS

Jorge Costa Lopes

Dissertação para obtenção do Grau de Mestre em

**Engenharia Electrotécnica e de Computadores**

**Área de Especialização de Automação e Sistemas**

Julho de 2008


# MONITORIZAÇÃO INTEGRADA PARA SISTEMAS DE ALIMENTAÇÃO DISTRIBUÍDOS

EFACEC – Sistemas de Electrónica, S.A.

Jorge Costa Lopes 1010904

Dissertação para obtenção do Grau de Mestre em

**Engenharia Electrotécnica e de Computadores**

**Área de Especialização de Automação e Sistemas**

Orientadora Interna: Prof.ª Benedita Malheiro
Orientador Externo: Eng.º Nuno Costa
Eng.º Nuno Delgado

Julho de 2008

«Dedico este trabalho à minha avó Isaura Jesus Vilar da Costa»

# Agradecimentos

Este trabalho não poderia ser desenvolvido sem o apoio de algumas pessoas, às quais deixo aqui os meus sinceros agradecimentos:

Ao Eng.º Nuno Costa da EFACEC Electrónica (Orientador Externo) pela orientação e aconselhamento que desenvolveu ao longo de todo o projecto. Sem a sua visão e aconselhamento técnico não seria possível desenvolver este projecto e atingir padrões de complexidade.

À Eng.ª Benedita Malheiro do ISEP (Orientadora Interna) pela orientação e aconselhamento que desenvolveu ao longo de todo o projecto. A sua ajuda e dedicação no desenvolvimento da Tese foi essencial para concluir este projecto com sucesso.

Ao Eng.º Nuno Delgado da EFACEC Electrónica pelo apoio ao nível da minha inserção no ambiente e organização da empresa.

Ao Eng.º Ricardo Barbosa da EFACEC Electrónica por disponibilizar uma parte integrante deste projecto e apoio dado na sua integração no projecto.

Queria igualmente estender os meus agradecimentos a todos os que me apoiaram, seja através da sua amizade ou de aconselhamento, durante esta fase, sendo alguns anónimos e outros bons amigos.

Um agradecimento especial ao meu pai, Florentino Lopes, mãe, Emília Rosa e irmão, Diogo Lopes, pelo apoio dado, sem o qual não seria possível embarcar neste projecto.

A todos o meu sincero muito obrigado.

# Resumo

O objectivo desta Tese/Dissertação é conceber um sistema para a **EFACEC – Sistemas de Electrónica, S.A.** que permita efectuar a monitorização, controlo e supervisão, de forma remota, de um vasto conjunto de equipamentos geograficamente distribuídos. Estes equipamentos são recursos críticos – Carregadores Industriais de Baterias (CIB) e Unidades de Alimentação Ininterrupta (UPS) – e requerem uma monitorização constante a fim de garantir uma elevada disponibilidade de serviço e, consequentemente, contribuir para a satisfação final do cliente.

Em primeiro lugar efectuou-se um estudo relativo à monitorização integrada de equipamentos geograficamente distribuídos para se determinar qual a arquitectura mais apropriada às necessidades do sistema e do mercado. O facto de, na maioria dos casos, se utilizarem as infra-estruturas físicas de comunicação já existentes facilita o seu desenvolvimento e evita efectuar grandes investimentos em telecomunicações. Adicionalmente, o tipo de controlo que estes sistemas atribuem a um operador, permite uniformizar e optimizar sistemas produtivos de forma a obter maiores margens de lucro, além de interligar quase todos os sectores de uma indústria.

Em segundo lugar concebeu-se a solução a realizar. Optou-se por uma aplicação *Web*, organizada em quatro camadas (navegador, servidor de aplicações, servidor de bases de dados e equipamentos remotos) destinadas a disponibilizar uma interface com o utilizador, implementar as funcionalidades necessárias para, em tempo real, recolher, armazenar e processar a informação dos equipamentos remotos. Dado que se decidiu dotar o sistema da capacidade de estabelecer ligações via Ethernet e modem com os equipamentos remotos, foi concebido um módulo específico dedicado ao estabelecimento destes tipos de ligações. Dado que o processamento de alarmes é uma actividade crítica do sistema, propôs-se a construção de um módulo adicional dedicado a esta actividade. Este módulo deverá incluir a capacidade de interrogar periodicamente todos os equipamentos sob monitorização e actualizar a base de dados do sistema. No seu todo, a aplicação

destina-se a permitir que um utilizador autorizado possa aceder ao sistema através de uma qualquer ligação à Internet para supervisionar o estado de todo os equipamentos remotos.

Seguiu-se o desenvolvimento do projecto, tendo-se implementado todos os módulos propostos. O conjunto de funcionalidades que possibilitam a supervisão remota dos equipamentos e que desencadeiam, sempre que necessário, a intervenção automática dos técnicos dos serviços de assistência foi realizado. A depuração da aplicação decorreu da realização de testes funcionais extensivos. No final, resultou um sistema com características e funcionalidades bastante atractivas para os clientes da EFACEC, permitindo explorar novas formas de gerir o sistema, optimizando a assistência e a monitorização, garantindo uma maior disponibilidade de serviço com redução de custos operacionais e cumprindo os objectivos propostos.

Por último, efectuou-se uma análise do impacto da adopção desta solução na empresa que permitiu constatar os benefícios decorrentes da sua utilização, tanto ao nível operacional como financeiro.

**Palavras-chave (Tema):** CIB, UPS, Sistema Distribuído de Monitorização; Controlo Remoto.

**Palavras-chave (Tecnologias):** SNMP, RS-232, Apache, MASON, Perl, AJAX, MySQL.

# Abstract

The aim of this Thesis / Dissertation is to devise a system for **EFACEC – Sistemas de Electrónica S.A.** to remotely control and supervise a large set of geographically distributed equipments. These equipments are critical resources – Switching Mode Rectifier Cabinets (CIB) and Uninterruptible Power Supplies (UPS) – that require constant monitoring to ensure a high availability of service to customers.

First, a study was carried out on integrated monitoring of distributed systems to determine the most appropriate architecture and to identify the requirements of both the system and market. Since, in most cases, a physical communications infrastructure is already available, it facilitates the development of these systems without the need for large communications investments. Additionally, such systems not only connect the distributed elements to a central office, but provide the operator with an overall type of control that allows the standardisation and optimisation of production systems, resulting in greater profit margins.

Secondly, a solution was designed. The proposed solution is a Web application, organized in four layers (client browser, application server, database server and remote equipments) aimed to provide a graphical interface to the end-user, implement all the features required to gather, store and process the information from the remote equipments. Since the application must communicate with the remote equipments, a communications module must be provided to establish connections via modem and via the Ethernet interface. An additional module, fully dedicated to alarm processing – a critical activity of this system – is also required. This module must periodically poll the set of remote equipments under supervision and update the database. The overall application is intended to provide authorised users with access to the distributed system through any Internet connection and, thus, monitor the state of all equipments.

During the project's development phase, the different modules were built. The set of functionalities that enable the monitoring of the remote equipments and that trigger, whenever necessary, the automatic intervention of assistance service were

developed. The application's debugging was made through the realisation of extensive functional tests. The resulting system includes very attractive features and functionalities for EFACEC's customers, providing new ways of managing remote equipments, optimizing the monitoring and assistance, ensuring greater availability of service and, thus, contributing to a reduction of operational costs and meeting the initial objectives.

Finally, the impact of the adoption of this solution was analysed and it was possible to identify the benefits of its use, at both operational and financial level.

**Key Words (Theme):** CIB, UPS, Distributed Supervision System, Remote Control.

**Key Words (Technologies):** SNMP, RS-232, Apache, MASON, Perl, AJAX, MySQL.

# Índice

# Índice de Figuras

# Índice de Tabelas

# Notação e Glossário

**3DES** *Triple Data Encryption Standard* - é um padrão de encriptação de dados baseado no algoritmo DES desenvolvido pela IBM em 1974.

***Addon*** É o nome que se dá a um recurso ou acessório que melhora ou aperfeiçoa a aplicação ao qual ele é acrescentado.

**ARP** *Address Resolution Protocol* - é um protocolo usado para encontrar um endereço Ethernet – *Media Access Control* (MAC) *address* – a partir do endereço IP.

**ASCII** *American Standard Code for Information Interchange* - é uma codificação de caracteres de sete bits baseada no alfabeto inglês

**AJAX** *Asynchronous Javascript And XML* - é o uso sistemático de tecnologias providenciadas por navegadores, como Javascript e XML, para tornar páginas mais interactivas com o cliente, fazendo uso de requisições assíncronas de informações.

**ATM** *Asynchronous Transfer Mode* - é uma arquitectura de rede de alta velocidade orientada a conexão e baseada na comutação de pacotes de dados.

**AP** *Access Point* - é um dispositivo de uma rede sem fios que realiza a conexão entre todos os dispositivos móveis.

***Bridge*** É o termo utilizado em informática para designar um dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos ou iguais ou dois segmentos da mesma rede que usam o mesmo protocolo.

**CaTV** Televisão por Cabo ou Televisão de Antena Comunitária por Cabo

***Cluster*** É um conjunto de computadores que se interligam através de um sistema não fragmentado. Tem por objectivo, dividir um certo processamento de dados com outras máquinas ligadas na mesma rede para acelerar o tempo total de processamento.

**CIB** Carregador Industrial de Baterias

**CRC** *Cyclic redundancy check* – (verificação de redundância cíclica) é um código detector de erros, um tipo de função que gera um valor expresso em poucos bits em função de um bloco maior de dados, como um pacote de dados, ou um ficheiro, de forma a detectar erros de transmissão ou armazenamento.

**Conitel** Protocolo desenvolvido para comunicação entre Sistemas SCADA e respectivos RTU do mesmo vendedor.

**DCS** *Distributed Control System* – Sistema de Controlo Distribuído

**DNP3** *Distributed Network Protocol* – Conjunto de protocolos de comunicação usado entre componentes em sistemas autónomos.

**DNS** *Domain Name System* – (Sistema de Nomes de Domínios) é um sistema de gestão e atribuição de nomes hierárquico.

**DHCP** É um protocolo que define um conjunto de regras usadas por dispositivos de comunicação tais como um *router* ou placa de rede, permitindo a estes dispositivos pedir e obter endereços IP de um servidor contendo uma lista de endereços disponíveis para atribuição.

**DB-9** É um tipo comum de conector, usado principalmente em computadores. Quando a porta série do PC começou a usar conectores de 9 pinos, ela foi baptizada de DB-9.

**DOM** *Document Object Model* - é uma especificação da W3C, independente de plataforma e linguagem, onde pode-se alterar e editar a estrutura de um documento electrónico. A API DOM oferece um modo padrão de aceder aos elementos de um documento, além de poder-se trabalhar com cada um desses elementos separadamente, e por esses motivos criar páginas altamente dinâmicas.

***Dial-Up*** É um tipo de acesso à Internet no qual uma pessoa usa um modem e uma linha telefónica para se ligar a um nó de uma rede de computadores do ISP.

***Ethernet*** É uma tecnologia de interligação para redes locais - *Local Area Networks* (LAN) - baseada no envio de pacotes.

***Firewall*** É um dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou recepção de dados nocivos ou não autorizados de uma rede para outra.

***Fork*** É uma ferramenta de programação que inicia uma bifurcação da execução de um processo, resultando desta operação um processo independente que executa em paralelo.

***Framework*** No desenvolvimento do *software*, um *framework* ou enquadramento é um ambiente integrado de suporte ao desenvolvimento de projectos de *software*. Um *framework* pode incluir programas de suporte, bibliotecas de código, linguagens de *scripting* e outros módulos para auxiliar no desenvolvimento e unir diferentes componentes de um projecto de *software*.

**FTP** *File Transfer Protocol*– é um protocolo de transferência de ficheiros através da Internet bastante rápido e versátil.

| | |
|---|---|
| ***Gateway*** | Um *Gateway*, ou *porta de ligação*, é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos. |
| **GPL** | *General Public License* - é a designação da licença para software livre idealizada por Richard Stallman no final da década de 1980, no âmbito do projecto GNU da Free Software Foundation (FSF). |
| **HMI** | *Human Machine Interface* – Interface Homem–Máquina. |
| **HTTP** | *HyperText Transfer Protocol* – Protocolo de transferência de Hipertexto |
| **HTML** | *HyperText Markup Language* - Linguagem de anotação de documentos. |
| **HP OpenView – Network Node Manager** | *Network Node Manager* (NNN) - é um produto de gestão de redes da OpenView do grupo Hewlett Packard. Este protocolo utiliza SNMP para comunicar com os componentes de uma rede, possibilitando a auto-descoberta, monitorização e controlo remotos. |
| **HTTPS** | *HyperText Transfer Protocol Secure* - é uma implementação do protocolo HTTP sobre uma camada SSL ou do TLS. Esta camada adicional permite que os dados sejam transmitidos através de uma conexão encriptada e verifica a autenticidade do servidor e do cliente através de certificados digitais. |
| **IP** | *Internet Protocol* - é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados. |
| **ISP** | *Internet Service Provider* – é um fornecedor de serviços que oferece acesso à Internet. |
| **IEC 61131-3** | Linguagem de programação com componentes gráficos para PLC. |

**IEC 60870-5** Protocolo que permite a conexão entre dois terminais permanentemente ligados para troca de informações de telecontrolo, usando pacotes de dados.

**IEC 61850** É um protocolo *standard* de automação para subestações.

**I2C** *Inter-Integrated Circuit* - é um barramento de comunicação série para computadores.

**ICMP** *Internet Control Message Protocol* - é um protocolo integrante do Protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original.

**Kernel** Núcleo de um sistema operativo ou, numa tradução literal, cerne. Ele representa a camada de *software* mais próxima do *hardware*, sendo responsável por gerir os recursos do sistema operativo como um todo.

**LED** *Light-Emitting Diode* – Díodo emissor de luz.

**LCD** *Liquid Crystal Display* - Ecrã de cristais líquidos.

**Linux** É o termo geralmente usado para designar qualquer sistema operativo que utilize o *kernel* Linux desenvolvido por Linus Torvalds.

**Lucent One Vision** *Software* de gestão de redes de comunicação desenvolvido pela Lucent.

**MAC** *Media Access Control* – é o endereço físico da interface de rede.

**Modbus** Protocolo de comunicação série desenvolvido pela Modicon para PLC.

**MTU** *Master Terminal Unit* – Unidade principal vulgo estação central.

***Multiplexer*** Um multiplexador, mux ou multiplexer é um dispositivo que codifica as informações de duas ou mais fontes de dados num único canal.

**NTP** *Network Time Protocol* - é um protocolo desenvolvido para permitir a sincronização dos relógios dos sistemas de uma rede de computadores.

***Overhead*** Em ciência da computação o *overhead* é geralmente considerado qualquer processamento ou armazenamento em excesso, seja de tempo de computação, de memória, de largura de faixa ou qualquer outro recurso que seja requerido para ser utilizado ou gasto para executar uma determinada tarefa.

**PDH** *Plesiochronous Digital Hierarchy* – é uma tecnologia de hierarquia digital para canais de comunicação onde ocorre multiplexação sucessiva usando-se TDM.

**PKI** *Public Key Infrastructure* - é um órgão ou iniciativa pública ou privada que tem como objectivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transacções entre partes que utilizam certificados digitais.

***Polling*** Processo de interrogação de diversos equipamentos de uma rede.

**Profibus** *Process Field Bus* – barramento de comunicações

**PLC** *Programmable Logic Controller* – Controlador lógico programável

***Plug-In*** É uma aplicação de computador (geralmente pequeno e leve) que serve normalmente para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica.

**PID** Um controlador PID é um controlador lógico que utiliza a proporcionalidade, integração e derivação para efectuar um controlo em malha fechada de um componente ou circuito

**PPPoE** *Point-to-Point Protocol over Ethernet* - é um protocolo para conexão de clientes a uma rede IP a Internet.

**PPP** *Point-To-Point Protocol* - é um protocolo que foi desenvolvido e padronizado através da RFC 1548 (1993) com o objectivo de transportar todo o tráfego entre 2 dispositivos de rede através de uma conexão física única.

***Prompt*** Nos sistemas operativos que dispõe de modo de linha de comando a *prompt* é constituída por um ou mais símbolos que indicam o local a partir do qual o utilizador deve digitar uma instrução num terminal de comandos.

**RFC-2217** *Telnet Com Port Control Option*

***Router*** É um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si.

**RTU** *Remote Terminal Unit* – Unidade remota constituída por um microprocessador controlado por telemetria

**RP-570** Protocolo de comunicação utilizado em ambientes industriais

**RC4** É o algoritmo de encriptação de fluxos de dados muito popular utilizado em protocolos, como SSL (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios).

**SCADA** *Supervisory Control And Data Acquisition* - Sistema de monitorização e controlo.

***Scripting Language*** É uma linguagem baseada em guiões/comandos que é interpretada linha a linha. Estes tipos de linguagens são executados por interpretadores específicos.

**SDH** *Synchronous Digital Hierarchy* - é um esquema de multiplexação TDM de faixa larga.

**SNMP** *Simple Network Management Protocol* – é um protocolo de gestão típico de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores.

**SMTP** *Simple Mail Transfer Protocol* - é o protocolo padrão para envio de *emails* através da Internet.

***Socket*** É o ponto terminal de uma comunicação bidireccional através de uma rede IP entre dois programas.

**SSH** *Secure Shell* - é, simultaneamente, 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.

**SMS** *Short Message Service* – Serviço de Mensagens Curtas.

**ODBC** *Open Data Base Connectivity* - é um padrão para acesso a servidores de bases de dados.

**OLE** *Object Linking and Embedding* - é um sistema de objectos distribuídos e um protocolo desenvolvido pela Microsoft.

**OSGi** *Open Services Gateway Initiative* - é uma plataforma de serviços para o desenvolvimento de aplicativos em Linguagem Java modulares e orientados a serviços.

**TDM** *Time-Division Multiplexing* – é um tipo de multiplexação, permite transmitir simultaneamente vários sinais, dentro do mesmo espaço físico (meio de transmissão), onde cada sinal (canal de comunicação), possui um tempo próprio e definido de uso da banda para transmissão.

**TCP/IP** Conjunto de protocolo de Internet que implementam um modelo por camadas para troca de dados.

**Telnet** é um protocolo cliente-servidor de comunicações usado para permitir a comunicação entre computadores ligados numa rede baseada em TCP.

**TCP** *Transmission Control Protocol* - é um protocolo do nível da camada de transporte (camada 4) do Modelo OSI e é sobre o qual assentam a maioria das aplicações cibernéticas, como o SSH, FTP, HTTP, a *World Wide Web*.

**TLS/SSL** *Transport Layer Security /Secure Socket Layer* - são protocolos de encriptação que fornecem comunicação segura na Internet para serviços como *email* (SMTP), navegação (HTTP) e outros tipos de transferência de dados.

***Trojan*** *Trojan Horse* é um programa que entra num computador e liberta uma porta para um possível invasor (vírus).

**UDP** *User Datagram Protocol* - significa Protocolo de Datagramas do Utilizador e faz a entrega de mensagens independentes, designadas por datagramas, entre aplicações ou processos, em sistemas *host*.

**Unix** Unix é um sistema operativo multitarefa e multiutilizador originalmente criado por Ken Thompson, que trabalhava nos Laboratórios Bell (Bell Labs) da AT&T.

**UPS** *Uninterruptible Power Supply* – Fonte ininterrupta de tensão DC.

**VPN** *Virtual Private Network* - é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

**XML** *eXtensible Markup Language* - É um subtipo de SGML (*Standard Generalized Markup Language*) ou Linguagem Padronizada de Marcação Genérica capaz de descrever diversos tipos de dados.

# 1 Introdução

## 1.1 Apresentação do Projecto/Estágio

A tese de Mestrado em Engenharia Electrotécnica – Área de Especialização em Automação e Sistemas foi elaborada no âmbito de um projecto desenvolvido na **EFACEC - Sistemas de Electrónica, S.A**. O projecto teve uma duração aproximada de um ano e foi desenvolvido no gabinete de Investigação e Desenvolvimento (I&D) da secção de Sistemas de Alimentação.

Teve como orientadores a Professora Benedita Malheiro por parte do Instituto Superior de Engenharia do Porto, Eng.º Nuno Costa e Eng.º Nuno Delgado por parte da EFACEC Sistemas de Electrónica, S.A.

### 1.1.1 Planeamento de Projecto

Este projecto foi organizado em quatro etapas. A primeira fase foi de estudo e investigação sobre o mercado e acerca dos equipamentos e soluções existentes no domínio da monitorização industrial distribuída. Esta análise foi utilizada para decidir qual a metodologia de desenvolvimento a adoptar e que tipo de soluções desenvolver.

Numa segunda fase, foram implementadas algumas das metodologias escolhidas. Na terceira fase procedeu-se a uma avaliação do impacto da adopção da solução desenvolvida. A quarta fase, que decorreu ao longo de todo o trabalho, consistiu na escrita desta dissertação.

### 1.1.2 Reuniões de Acompanhamento

As reuniões de acompanhamento que ocorreram ao longo deste trabalho são apresentadas de seguida sob a forma de tabela, onde se descrimina o dia, tema e intervenientes (excluindo o candidato).

Tabela 1 - Tabela de reuniões de acompanhamento com Orientadores do Mestrado

| *Data da Reunião* | *Intervenientes* | *Tema debatido* |
|---|---|---|
| 24/09/2007 | Eng.º Nuno Costa<br>Eng.º Nuno Delgado | Análise a propostas de projecto |
| 28/09/2007 | Eng.º Nuno Costa | Definição do projecto |
| 01/10/2007 | Eng.º Nuno Costa | Definição de requisitos e funcionalidades gerais |
| 12/10/2007 | Eng.º Nuno Costa | Acompanhamento de pesquisa |
| 29/11/2007 | Prof.ª Benedita Malheiro | Delineação de linhas de orientação |
| 04/12/2007 | Eng.º Nuno Costa | Análise de *software* de gestão / características a desenvolver no sistema |
| 13/12/2007 | Eng.º Nuno Costa | Análise de protocolos de Comunicação / Gestão de alarmes |
| 17/12/2007 | Eng.º Nuno Costa | Definições de estruturas modelares |
| 18/06/2008 | Eng.º Nuno Costa | Definição de metas finais do desenvolvimento |
| 20/06/2008 | Prof.ª Benedita Malheiro | Definição de elementos finais da tese |

## 1.2 Organização do Relatório

Este relatório é composto por um estudo da área de monitorização da EFACEC para conhecer quais os equipamentos existentes, soluções e tecnologias utilizadas, assim como quais as mais recentes tendências no domínio da monitorização industrial.

É apresentada uma solução, descrito o *hardware* utilizado e o *software* desenvolvido. As funcionalidades do projecto são apresentadas, seguidas de uma conclusão, onde se apresenta um estudo do impacto da adopção da ferramenta desenvolvida, e de uma proposta de enriquecimentos.

## 1.3 Estado do Conhecimento e Tecnologias Utilizadas

A presente Tese/Dissertação abrange uma área importante da monitorização distribuída na indústria. Tradicionalmente, neste domínio, recorre-se a sistemas SCADA e protocolos de comunicação padrão para interligar equipamentos remotos. Neste contexto irão ser analisados este tipo de sistemas e estudado o problema de aquisição e controlo de componentes electrónicos industriais em rede, particularizando-se as soluções que o mercado disponibiliza. A solução a adoptar no projecto deverá assegurar a troca de informação, a estabilidade e minimizar o custo associado à sua exploração.

## 1.4 Apresentação da Organização

O Grupo EFACEC é o maior grupo electromecânico nacional de capitais portugueses, com elevada expressão em diversos mercados internacionais. Subdivide-se em áreas tais como Transportes, Logística, Ambiente, Energia, Indústria e Edifícios, Telecomunicações e Serviços.

Com mais de 100 anos de história, o Grupo EFACEC teve a sua origem na "Moderna", empresa nascida em 1905. Constituída em 1948, a EFACEC, enquanto maior Grupo Eléctrico Nacional de capitais portugueses, tem cerca de 2000 colaboradores e factura aproximadamente 300 milhões de Euros, estando presente em mais de meia centena de países e exportando cerca de metade da sua produção [1].

O *portfolio* de actividades da EFACEC, recentemente reorganizado, divide-se em:

- Soluções para Energia
- Soluções para Transportes e Logística
- Soluções de Engenharia e Serviços**,**

sustenta uma abordagem cada vez mais sistémica/integradora, satisfazendo as necessidades actuais do mercado e rentabilizando as várias valências do Grupo.

A aposta da EFACEC no mercado Internacional, bem como um forte investimento na Inovação e no desenvolvimento de novas tecnologias, em articulação com as tecnologias de base, fazem com que a EFACEC tenha sabido penetrar favoravelmente no mercado, posicionando-a na linha da frente da indústria portuguesa e nos mercados internacionais.

Estes factores são a base para o crescimento e desenvolvimento sustentados do Grupo EFACEC [1].

A EFACEC Sistemas de Electrónica, Unidade de Sistemas de Alimentação é a empresa onde se desenvolveu o projecto e é, dentro do Grupo EFACEC, a unidade responsável pela produção de sistemas de alimentação (UPS e rectificadores principalmente para centrais de telecomunicações, subestações de energia, *etc.*) e conversores de potência (rectificadores de tracção, inversores), tendo competências também ao nível da electrónica de sinal e *software* utilizados no desenvolvimento de PSM para os seus Carregadores Industriais de Baterias (CIB) [2].


Figura 1 – Instalações da EFACEC Sistemas de Electrónica S.A.

## 1.5 Contexto

Pretende-se desenvolver um estudo e apresentar uma solução técnica para um produto da EFACEC – Sistemas de Electrónica, de forma ir de encontro às necessidades e exigências específicas dos clientes e do mercado.

Para os CIB e UPS da EFACEC, desenvolvidos e produzidos pela Secção de Alimentação, é necessário desenvolver uma aplicação servidora que permita integrar a informação de diversos equipamentos, efectuar a sua monitorização e controlo. Estes equipamentos constituem recursos críticos dos clientes da empresa e requerem uma monitorização constante a fim de garantir uma elevada

disponibilidade de serviço. Será efectuado um estudo das funcionalidades a implementar para que o produto vá ao encontro das necessidades dos clientes e será feita uma pesquisa às soluções que o mercado oferece neste âmbito. O servidor deverá ser capaz de integrar a informação de vários CIB e UPS, permitindo a monitorização remota e controlo dos mesmos tanto através de um serviço fornecido sobre HTTP, adaptável a todos os navegadores *Web*, como através do protocolo SNMP. Deverá ainda ser possível ao sistema gerar e enviar alertas de mau funcionamento de componentes através de *email* e de SMS. Os dados relativos ao histórico do funcionamento dos equipamentos deverá estar disponível em base de dados. Deverá, igualmente, ser possível estabelecer ligações entre os diversos equipamentos a monitorar e a plataforma de aplicação servidora via interface Ethernet e modem analógico.


Figura 2 – Bastidor CIB

A partir do estudo dos requisitos do sistema e da extensa pesquisa das soluções existentes no mercado serão determinadas as características necessárias para o produto a desenvolver. A solução encontrada deverá ir de encontro às necessidades específicas dos clientes e do mercado em que se insere.

# 2 Estado da Arte

## 2.1 Evolução da Automação na Indústria

Desde sempre a indústria tentou optimizar questões relacionadas com a troca de informação entre as diversas máquinas e componentes e os seus respectivos operadores. Com o crescimento do número de máquinas e aumento das suas capacidades, também a quantidade de informação e respectiva especificidade aumentaram, colocando sobre o operador maior responsabilidade. De forma a aumentar a capacidade de resposta ao aumento da complexidade dos processos fabris, a indústria respondeu com a digitalização e integração dos diversos sistemas.

A integração de microcontroladores em praticamente todas as máquinas industriais permitiu dotá-las de uma capacidade de monitorização e controlo sem precedentes. Passou a ser possível a um operador obter informação precisa e actual sobre o estado de uma máquina e seu respectivo funcionamento, assim como sobre o produto em fabrico. Através de indicações visuais tais como LED ou ecrãs LCD estas máquinas são capazes de informar o operador de eventuais problemas no seu funcionamento, através de alarmes, e, inclusive, podem ser reprogramadas. Este avanço permitiu reduzir o número de operadores necessários para cada máquina, cabendo-lhes agora as tarefas de monitorização, controlo e reprogramação.

O passo seguinte consistiu na interligação de diversas máquinas, automatizando desta forma o processo produtivo. A criação de redes de máquinas levantou novas questões que, até esta altura, não haviam sido colocadas. Questões como qual o protocolo de ligação a utilizar de forma a escudar a linha a ruídos externos, qual a hierarquia das máquinas e se haveria controlador central, qual a informação primária, vital e a informação secundária, questões de segurança das máquinas e dos operadores, questão da segurança da rede quando integradas com redes externas ou questões relacionadas com o controlo das próprias máquinas.

Nasceu assim a era da Automação na Indústria que levou ao desenvolvimento de sistemas que integram todas as máquinas de uma unidade industrial, interligando-as entre si, e levando a que poucos operadores (altamente qualificados) sejam capazes de gerir uma secção de produção. Para tal foi necessário criar redes informáticas versáteis capazes de dar resposta às exigências deste tipo de ambiente. Foram criados dois conceitos de monitorização e controlo de sistemas distribuídos na indústria: o SCADA e o DCS.

De forma a definir qual o tipo de arquitectura de sistema mais apropriado ao desenvolvimento deste projecto (na perspectiva de integração em rede), serão apresentadas e comparadas as arquitecturas dos sistemas SCADA e DCS.

## 2.2 SCADA

A resposta para a integração da rede de controladores de máquinas industriais (PLC, microcontroladores, *etc.*) surge pela mão do SCADA. SCADA é o acrónimo de *Supervisory Control And Data Acquisition* e refere-se a um sistema de aquisição de dados e controlo. Os sistemas SCADA são sistemas tipicamente utilizados para efectuar a recolha de dados enviados pelas diferentes máquinas integrantes de um sistema e efectuar o seu controlo a um determinado nível.

O sistema de supervisão assenta sobre um sistema de controlo em tempo real para controlar um processo que é externo ao próprio sistema de SCADA. Por outras palavras e a título ilustrativo, um computador não é, em si mesmo, um sistema SCADA apesar de controlar o seu próprio consumo de energia e arrefecimento. Isto implica que o sistema não é crítico no controlo do processo em tempo real dado existir um sistema de controlo (automatizado e de tempo real) separado ou integrado com a máquina na qual ocorre o processo, de forma a compensar as variações com velocidade suficiente. O papel a desempenhar por esse sistema integrado é normalmente feito pelo microcontrolador ou PLC associado a cada máquina.

Os tipos de processos para o qual o sistema SCADA foi desenvolvido englobam:

- Industrias tais como a manufactura, produção, geração de energia, fabricação e refinamento através de processos contínuos, repetitivos ou discretos;

- Infra-estruturas públicas ou privadas tais como tratamento e distribuição de água, recolha e tratamento de resíduos fluviais, gasodutos e condutas de petróleo, linhas de transmissão e distribuição de energia eléctrica e grandes sistemas de comunicações;

- Controlo e gestão de acesso e/ou energia para edifícios, aeroportos, navios ou estações espaciais.

Os sistemas de SCADA desenvolvidos para cada um destes tipos de aplicações são muito diferentes entre si, embora façam uso dos mesmos conceitos básicos de controlo e monitorização.

### 2.2.1 Conceito do Sistema

Um sistema SCADA inclui, na sua globalidade, *hardware* de entradas e saídas de sinal (digital e/ou analógico), controladores, Interface Homem-Máquina – *Human-Machine Interaction* (HMI), redes, comunicações, bases de dados e *software*. Normalmente, vem com um conjunto de soluções de Engenharia de Instrumentação específico para cada aplicação para o qual foi desenvolvido.

A utilização do termo SCADA aplica-se normalmente em relação ao sistema central que monitoriza e controla uma área industrial completa ou vários sistemas espalhados por uma longa distância. Consiste numa ou mais unidades principais – *Master Terminal Units* (MTU) – que um operador utiliza para controlar as diversas unidades remotas – *Remote Terminal Units* (RTU). Este sistema utiliza, na maioria das vezes, o mesmo suporte físico e protocolo de comunicação que as redes LAN [3].

O controlo local sobre a máquina é efectivamente feito pela RTU ou por um PLC. As acções de controlo do controlador local estão quase sempre restringidas a níveis de supervisão e controlo sobre níveis de funcionamento da máquina. Por exemplo, um PLC pode controlar o fluxo de água para arrefecimento de uma máquina como parte do processo industrial, mas o SCADA pode permitir ao operador

modificar o nível de referência do fluxo e permitir que qualquer alarme relativo à diminuição do caudal ou alta temperatura seja mostrado e gravado. O ciclo de controlo de uma máquina é imposto pela resposta a um evento ou a uma medida feita pela RTU ou PLC local, enquanto que o SCADA supervisiona o desempenho desse ciclo e permite a parametrização do mesmo.

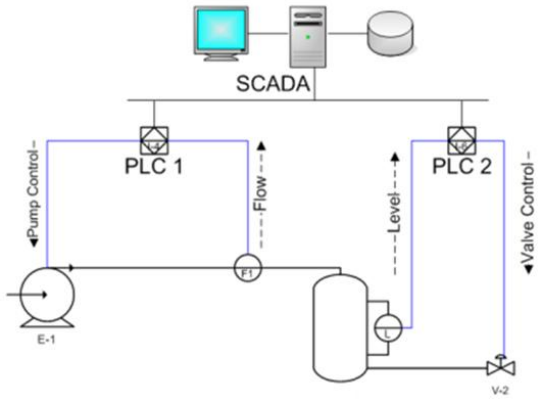


Figura 3 – Exemplo de SCADA

A aquisição de dados começa ao nível da RTU ou do PLC e inclui medições e estado dos diversos equipamentos que são comunicados ao sistema central do SCADA assim que forem requisitados. A informação é então compilada e formatada de forma a que o operador, através da HMI, seja capaz de tomar as devidas medidas de supervisão que possam ser necessárias para garantir o normal funcionamento do equipamento ou processo produtivo. A informação pode também ser colectada num histórico adequado, normalmente depositada num Sistema de Gestão de Informação, para permitir a realização de análises analíticas do desempenho do sistema e equipamentos.

Os sistemas SCADA normalmente implementam uma base de dados distribuída, normalmente referida como *tag database* que contém elementos chamados *tags* (marca ou anotações) ou *points* (pontos). Um ponto representa um único valor de entrada ou de saída que é monitorizado ou controlado pelo sistema. Os pontos podem ser "*hard*" ou "*soft*". Um ponto *hard* representa um valor real de entrada ou saída do sistema, enquanto que um ponto *soft* é o resultado de operações lógicas ou matemáticas aplicadas sobre outros pontos, tanto *hard* como

*soft*. A maioria das implementações remove esta distinção fazendo com que todos os pontos sejam *soft.* A informação relativa a estes pontos é guardada no histórico, sendo associada a uma escala temporal. É também habitual guardar informação adicional tal como o endereçamento da RTU que registou o valor, informação de alarmes e comentários.

### 2.2.2 Interface Homem-Máquina

O HMI, acrónimo de *Human-Machine Interface*, é o modo ou interface como a informação é apresentada ao operador e através da qual o operador controla o processo constitui a interface com o utilizador.

O desenvolvimento da HMI neste contexto resultou da necessidade de padronizar a forma de apresentar, monitorizar e controlar os múltiplos controladores remotos, PLC e outros aparelhos de controlo. A informação é recolhida pelos vários controladores através da rede, processada e apresentada ao operador. O módulo HMI pode também ser ligado uma base de dados para que possa fornecer informação de diagnóstico e executar procedimentos de manutenção pré-programados, fornecer dados de logística, fornecer esquemas de máquinas ou sensores e guias de resolução de problemas especialmente concebidos para situações específicas. Desde 1998 todos os fabricantes de controladores fornecem sistemas integrados de HMI/SCADA, muitos deles utilizando protocolos de comunicação *open source*.

Existem numerosos pacotes adicionais para sistemas HMI/SCADA, muito dos quais são compatíveis com a maioria dos PLC, permitindo a engenheiros mecânicos, electrotécnicos e técnicos a configuração de HMI sem a necessidade de desenvolver *software* específico.

O SCADA é popular devido à sua compatibilidade e fiabilidade. É utilizado tanto em pequenas aplicações, tais como o controlo da temperatura de uma sala, como em grandes aplicações tais como o controlo de centrais nucleares.

### 2.2.3 Soluções de *Hardware*

As distribuições de SCADA são normalmente acompanhadas por sistemas distribuídos de controlo – *Distributed Control Systems* (DCS) – dado que a utilização de RTU e PLC capazes de autonomamente executar operações lógicas sem o envolvimento de um computador central está a aumentar. Uma linguagem de programação, IEC-61131-3, é regularmente utilizada para criar os programas que são executados nesses RTU e PLC. O IEC 61131-3, ao contrário de linguagens como C ou FORTRAN, necessita de pouca formação para se aprender a dominar a linguagem, permitindo que os engenheiros do sistema SCADA afectem o *design* e implementação de programas para serem executados nos RTU ou PLC.

### 2.2.4 Componentes do Sistema

Os três principais componentes de um sistema SCADA são:

- Múltiplas RTU;
- Computadores de Estação Central e HMI;
- Estrutura de comunicação;

#### 2.2.4.1 Terminais Remotos

A unidade terminal remota – *Remote Terminal Unit* (RTU) – liga-se ao equipamento físico remoto (máquina ou componente), faz a leitura de dados de estados tais como o estado aberto/fechado de um interruptor ou válvula, efectua a medição de valores tais como a pressão, fluxo, tensão ou corrente. Através do envio de sinais digitais para os equipamentos de RTU é possível controlar o equipamento através de operações tais como abrir ou fechar válvulas ou adoptar um novo valor para uma tensão. As RTU podem medir dados em formato analógico ou digital e enviar comandos digitais ou medidas digitais.

Uma implementação importante na maioria dos sistemas SCADA são os alarmes. Um alarme é um estado digital que tanto pode ter o valor *NORMAL* ou *ALARM*. Os alarmes podem ser criados de tal maneira que, quando se verificarem

determinadas condições, são activados. Um exemplo de um alarme é a luz de indicação de tanque de gasolina vazio num automóvel. A atenção de um operador de SCADA é atraída para a parte do sistema que activou o alarme. É possível configurar um sistema SCADA para o envio de *emails* e SMS para o operador e/ou administrador do sistema de forma a alertá-lo para a ocorrência de um alarme e do mau funcionamento do equipamento ou sistema.

#### 2.2.4.2 Estação Central

O termo Estação Central ou *Master Station* refere-se aos servidores e ao *software* responsável pela comunicação com o equipamento de campo (RTU, PLC, *etc.*) e o *software* de HMI a ser executado nas salas de controlo. Em pequenos sistemas de SCADA, a estação central pode incluir vários servidores, aplicações de *software* distribuídas e aplicações de recuperação de dados após mau funcionamento.

Os sistemas SCADA, normalmente, apresentam a informação para o pessoal operacional através de elementos gráficos sob a forma de um gráfico minimalista. Isto significa que o operador observa um esquema representativo da planta do sistema a ser controlado. Por exemplo, uma imagem de uma bomba pode fornecer o nível de fluído que a atravessa num determinado momento. O operador pode então desligar a bomba se o nível atingir valores críticos. O *software* de HMI permite ver o fluxo de fluído que atravessa a bomba em tempo real. Os gráficos minimalistas consistem em linhas gráficas e símbolos esquemáticos para representar elementos do sistema ou podem consistir em fotos digitais do equipamento sobrepostas por elementos gráficos animados que simbolizem o estado do equipamento.

Os pacotes de HMI para os sistemas SCADA incluem tipicamente um programa de desenho que permite aos operadores ou pessoal de manutenção do sistema modificar a forma como estes elementos visuais são apresentados no sistema. Inicialmente, plataformas *open source* tais como o Linux não eram utilizadas devido ao ambiente dinâmico em que eram desenvolvidas e porque para os componentes a ser controlados podiam necessitar de licenças UNIX e OpenVMS e partilhar o código desenvolvido. Hoje em dia, as estações HMI e estação central são disponibilizadas para a maioria dos sistemas operativos.

### 2.2.5 Filosofia Operacional

Em vez de confiar na intervenção de um operador ou nos automatismos da estação central, o RTU poderá estar configurado para efectuar o seu próprio controlo assim que ocorra um dado evento na máquina que controla. À estação central compete efectuar uma análise mais cuidada à informação que recebe, filtrar os dados relevantes e apresentá-los ao operador, incluindo uma análise histórica e uma análise associada aos requisitos de um sector industrial em particular. Os requisitos de segurança estão actualmente a ser associados ao sistema como um todo, incluindo até o *software* das estações centrais que deve cumprir os *standards* exigidos por alguns mercados.

Para algumas instalações o custo que resultaria da falha do sistema de controlo seria extremamente alto, podendo até incluir a perda de vidas humanas. Para colmatar esse problema, o *hardware* dos sistemas SCADA é geralmente desenhado para aguentar temperaturas altas, vibração e tensões extremas, sendo a fiabilidade destes sistemas aumentada através da redundância no *hardware* e nos canais de comunicação. Um componente que apresente uma falha pode ser rapidamente identificado e as suas funcionalidades rapidamente retomadas pelo sistema de apoio. Dessa forma, a parte defeituosa pode ser reparada ou substituída sem haver a necessidade de interromper o processo. A fiabilidade deste tipo de sistemas pode ser calculada estatisticamente, nomeadamente o tempo mínimo entre falhas que chega a rondar os séculos.

### 2.2.6 Infra-estrutura de Comunicação e Métodos

Os sistemas SCADA utilizam normalmente combinações de ligações via rádio e conexões via modem para estabelecerem a comunicação com os elementos remotos a controlar. Actualmente, a Internet é também frequentemente utilizada em grandes domínios tais como nas empresas ferroviárias e estações de produção de energia. Esta distinção de métodos de comunicação também vem ao encontro de alguns requisitos dos clientes que desejam utilizar a infra-estrutura já instalada no seu ambiente corporativo e/ou partilhar a rede com outras aplicações.

Dada a panóplia de equipamentos passíveis de monitorização, os protocolos antigos de faixa estreita continua a ser implementados em sistemas SCADA modernos. Estes sistemas são projectados para serem muito compactos e, alguns, são desenhados para que os dados apenas sejam enviados dos RTU para a estação central a pedido desta. Este método, embora leve a um menor fluxo de informação, descongestiona o canal de comunicação, o que em algumas redes é vital. Alguns destes protocolos antigos ainda suportados incluem o Modbus, RP-570 e Conitel, que são protocolos de comunicação específicos de cada fornecedor de SCADA. Os protocolos *standard* são o IEC 680870-5-101 ou 104, IEC 61850, Profibus e DNP3. Muitos destes protocolos contêm já extensões que lhes permitem operar sobre redes TCP/IP, embora seja boa prática de segurança de engenharia evitar ligar estes sistemas directamente à Internet para diminuir o risco de ataques ao sistema.

Dado que um grande número de vendedores continua a criar o seu próprio protocolo de comunicação (protocolo proprietário) com o intuito de fidelizar a sua base de clientes, as RTU e outros componentes de controlo estão actualmente a ser desenvolvidos de forma a garantir a interoperacionalidade entre *standards* da indústria. Módulos como o Modbus TCP/IP estão a ter grande aceitação no mercado e são já uma referência para muitos fabricantes de sistemas SCADA.

### 2.2.7 Rumo de Desenvolvimento do SCADA

A tendência é que o *software* dos PLC e HMI/SCADA esteja cada vez mais interligado. Nos inícios dos anos 90, o fabricante típico de componentes de controlo oferecia o seu próprio protocolo de comunicação que era suportado por protocolos físicos de longa distância como o RS-485. Nos finais dos anos 90, a transição para protocolos abertos de comunicação começou a ocorrer com os fabricantes a oferecer suporte para Modicon MODBUS sobre RS-485. Por volta de 2000, a maioria dos fabricantes de interfaces de I/O ofereciam uma interface aberta do tipo Modicon MODBUS sobre TCP/IP. As principais barreiras à entrada do TCP/IP no mercado da automação industrial têm vindo a ser ultrapassados pelos fornecedores de SCADA e prendiam-se com o determinismo, sincronismo, selecção do protocolo e adaptabilidade ao ambiente industrial.

Recentemente a segurança dos sistemas baseados em SCADA tem sido colocada em causa pelo aumento de ataques de *software* malicioso e de piratas informáticos em várias frentes. Em particular, os investigadores de segurança identificaram os seguintes problemas:

- A baixa preocupação existente acerca da segurança e autenticação no desenho, desenvolvimento e utilização de sistema SCADA existentes;

- A crença errónea que os sistemas SCADA beneficiam de "segurança por obscuridade" através do uso de protocolos especializados e de interfaces proprietárias;

- A crença errónea que as redes de SCADA são seguras porque são, supostamente, fisicamente seguras;

- A crença errónea que as redes SCADA estão supostamente desligadas da Internet.

Devido à natureza crítica da missão de certos sistemas SCADA, tais ataques poderiam, no pior cenário, causar uma enorme perda financeira através da destruição de dados ou de *hardware* ou até mesmo a perda de vidas. Algumas empresas, no intuito de desenvolver uma solução para este problema, começaram a desenvolver linhas de *firewall* industriais e soluções de VPN para sistemas SCADA baseados em redes TCP/IP [4].

## 2.3 Sistemas de Controlo Distribuído

Os sistemas de controlo distribuído – *Distributed Control Systems* (DCS) – são sistemas compostos por elementos de controlo geograficamente distribuídos, podendo cada componente do subsistema ser controlado por um ou mais controladores. O conjunto de controladores encontra-se ligado através de uma rede de comunicação e monitorização.

Os DCS são utilizados em variadas indústrias para a monitorização e controlo distribuído de equipamentos, tal como em centrais de geração de energia, sistemas

de controlo ambiental, sinais de tráfego, sistemas de distribuição de águas, refinarias de petróleo, fábricas de produtos químicos, indústria farmacêutica, redes de sensores e indústria naval.

### 2.3.1 Elementos

O DCS utiliza computadores como controladores (normalmente com processadores projectados especialmente para esta função) e usa tanto protocolos proprietários como protocolos *open source* para a interligação das várias partes do sistema. Os módulos de entrada e saída de dados são partes constituintes do sistema DCS. O processador recebe informação das entradas de dados e envia informação para a saída de dados dos módulos. Os módulos de entrada de dados recebem informação de instrumentação de medida na área de produção e os módulos de saída de dados transmitem instruções para os instrumentos de saída. No fundo, actuam como uma interface entre o processador e os actuadores sobre o sistema. As redes de computadores ou redes eléctricas ligam o processador e os módulos através de *multiplexers/demultiplexers*. Estas redes também interligam os controladores distribuídos ao controlador central e, por fim, ao HMI ou consola de controlo.

Os elementos de um sistema distribuído de controlo podem ligar-se directamente ao equipamento físico, tal como interruptores, bombas e válvulas ou podem operar através de um sistema intermediário como o SCADA.

### 2.3.2 Aplicações

Os sistemas DCS são sistemas dedicados utilizados para controlar processos produtivos que são contínuos ou orientados ao produto, tais como as refinarias de petróleo, petroquímicas, centrais de produção de energia, farmacêuticas, produção de alimentos, produção de cimento, produção de aço e fabrico de derivados de papel. Os DCS são conectados a sensores e actuadores e utilizam um controlo de nível para controlar o fluxo de material através da fábrica. O exemplo mais comum de um ciclo de nível de controlo é o de um sensor de pressão, controlador e uma válvula de controlo. As medições de pressão ou fluxo são transmitidas ao controlador, normalmente através de condicionamento de sinal para um

componente de interface de entradas e saídas de dados (I/O). Quando as variáveis medidas atingem um certo ponto, o controlador instrui a válvula ou actuador para abrir ou fechar de forma a que o fluído regresse ao seu fluxo normal. Grandes refinarias de petróleo têm centenas de pontos de I/O e utilizam grandes sistemas DCS.

O típico DCS consiste num conjunto de controladores funcionais e/ou distribuídos geograficamente capazes de executar de 1 a 256 ou mais ciclos de controlo regulador numa caixa de controlo. Os componentes de entrada e saída de dados (I/O) podem ser integrados com o controlador ou localizados remotamente através de uma rede local. Hoje em dia, os controladores têm uma capacidade computacional que excede largamente a capacidade de efectuar operações lógicas através do controlo de proporcionalidade, integração e derivação, típica nos PID.

Um sistema DCS pode ter uma ou várias estações de trabalho e pode ser configurado numa estação ou num PC. A comunicação local é controlada por uma rede de controlo através de cabos de par entrançado, coaxial ou fibras ópticas. Um servidor e/ou processadores de aplicações podem estar incluídos no sistema para computação adicional e armazenamento de informação.

## 2.4 Vantagens Económicas de Sistemas de Monitorização Remota

O elevado custo de desenvolvimento e aquisição de um sistema de monitorização integrada acarreta uma tomada de decisão importante para qualquer empresa. Quais as potenciais vantagens que um sistemas deste tipo poderá trazer para uma organização? Será o investimento neste tipo de produto absolutamente necessário?

A resposta a estas questão varia de produto para produto, de organização para organização. Há de facto sectores onde a implementação deste tipo de sistema não fará muito sentido. Pequenas empresas com poucos componentes a controlar e monitorizar, sobre uma área pequena, poderão dispensar este tipo de tecnologia. A vigilância constante de uma máquina (ou conjunto de máquinas) por parte de um operador poderá ser mais que suficiente para garantir o seu correcto

funcionamento. Isto deve-se, em parte, ao desenvolvimento dos controladores directos sobre as máquinas (ou componentes) que têm vindo a aumentar a capacidade de monitorização e controlo em malha fechada. Este tipo de controlo encontra-se já suficientemente desenvolvido e com poder de computação suficiente para ser autónomo no controlo da máquina, responder rápida e eficazmente a um evento e garantir alguma estabilidade. Com uma supervisão relativamente constante de um operador, estes sistemas garantem a fiabilidade suficiente para muitos casos.

Claro que este tipo de suposição parte do princípio que estes equipamentos não sejam vitais e que a sua falha não compromete nem equipamentos nem vidas humanas, *i.e*., são, geralmente, equipamentos secundários de uma indústria. Nestes casos, a aplicação de um sistema de monitorização e controlo poderá ser um investimento que apenas compense a longo prazo ou nem chegue sequer a compensar. Isto deve-se ao facto de, além do custo da aquisição do equipamento, instalação e treino do operador, haverá ainda os custos relativos à sua manutenção. Para que o investimento no sistema compensasse, a empresa teria que (entre outras situações):

- Ter um custo de manutenção do sistema de monitorização integrada e de um operador inferior ao custo de uma equipa de operadores;

- Verificar uma redução no número de falhas das máquinas (devido ao controlo mais apertado e actuação mais rápida sobre a máquina) ao ponto de baixar os respectivos custos de manutenção;

- Verificar um aumento da produtividade resultante do controlo mais rápido das máquinas.

Se para pequenas organizações, com sistemas pequenos e não vitais, a aquisição de um sistema de monitorização e controlo se possa colocar ainda como opção, para organizações ou indústrias com sistemas distribuídos de muito maiores dimensões, a aquisição deste tipo de equipamento é vital. Desde logo esta indústria debate-se com questões básicas:

- Como monitorizar e controlar conjuntos de equipamentos que podem chegar às centenas ou mesmo milhares?

- Como monitorizar e controlar equipamentos espalhados por grandes áreas geográficas?

- Como ter acesso imediato a equipamentos de forma a activar sistemas de apoio rapidamente em caso de falha de sistemas principais?

- Como garantir a estabilidade e harmonia no funcionamento de todo o sistema industrial?

- Como reduzir custos relativos à mão-de-obra necessária para a manutenção de componentes de uma grande área industrial?

- Como evitar deslocações desnecessárias a equipamentos instalados em locais remotos, optimizando o seu funcionamento?

Para este tipo de questões os sistemas de monitorização e controlo são a resposta mais atractiva. O facto de, na maioria dos casos, utilizarem como infra-estruturas físicas de comunicação as infra-estruturas já existentes (ligações via Ethernet, por exemplo) facilita a sua implementação, remetendo a maior fatia do custo de implementação deste tipo de sistemas para o desenvolvimento dos módulos próprios necessários para cada empresa. De facto, o controlo que um operador deste tipo de sistemas tem sobre a instalação permite uniformizar e optimizar os sistemas produtivos, resultando na obtenção de maiores margens de lucro.

Os sistemas de monitorização e controlo de sistemas distribuídos tornam-se, em alguns casos, a espinha dorsal de uma indústria, sem os quais esta não poderia evoluir. Contribuem, indirectamente, para a diminuição dos custos de produção em muitas empresas e conferem mais qualidade a cada produto, através de sistemas integrados de testes de monitorização de produtos finais. No caso de empresas que têm equipamentos distribuídos por grandes áreas geográficas e de difícil acesso (como as células de rede de empresas de telecomunicações móveis), a utilização

deste tipo de sistemas para interligar todos os equipamentos e monitorizar o seu funcionamento torna-se absolutamente vital. É o caso de equipamentos como os CIB, que são instalados em muitas células de redes de telecomunicações. A inclusão deste tipo de sistemas permite que técnicos localizados num posto de trabalho remoto operem sobre estes equipamentos, procedendo a reconfigurações e testes de rotina. Isto leva a uma redução significativa de custos relativos a deslocações dado que a periodicidade com que o técnico terá que se deslocar ao local será bastante reduzida. Mais uma vez, em termos económicos, os sistemas de controlo e monitorização de sistemas distribuídos apresentam vantagens pois permitem uma redução na mão-de-obra necessária para efectuar a manutenção do sistema e a redução dos custos de deslocação. Esta redução nos custo poderá reflectir-se sobre os lucros da empresa ou na diminuição dos custos de serviço e/ou produtos, levando a um aumento de competitividade no mercado em que se insere.

## 2.5 Soluções de Fabricantes de CIB

Até agora foi apresentada a perspectiva geral de interligação dos sistemas a supervisionar. Esta perspectiva ajuda a compreender a dinâmica e hierarquia da troca de dados entre os sistemas, desde o componente que se deseja controlar até ao operador. Desde logo define três níveis bem distintos:

- Componente ou máquina que executa as funcionalidades;
- Controlador directo do componente ou máquina;
- Controlador geral do sistema.

Em termos práticos, no caso em estudo, o componente ou máquina que executa as funcionalidades é o próprio CIB. O controlador directo do componente ou máquina é um PLC – *Programmable Logic Control* - ou microcontrolador que está programado para reagir a variações dos parâmetros de funcionamento da máquina, actuando sobre esta num circuito de compensação em malha fechada ou enviando alertas para o controlador do sistema. Este controlador directo é um controlador local pois controla apenas uma máquina ou componente. O controlador geral do

sistema será responsável por monitorizar e controlar um conjunto de controladores directos. Este controlador será a interface entre o administrador e/ou operador e o conjunto de máquinas que controla.

Conhecida esta estrutura, o estudo será desenvolvido sobre a perspectiva do controlador geral (no qual se integra o produto desenvolvido no projecto), interacção entre este e o controlador directo, protocolos e tecnologias utilizadas, funcionalidades disponibilizadas e soluções de mercado.

Esta abordagem passa por analisar como é que os fabricantes fazem esta distinção e que tipo de produtos disponibilizam para possibilitarem a monitorização integrada de sistemas distribuídos.

### 2.5.1 Controladores de CIB

Cada fabricante de CIB fornece um controlador especialmente desenvolvido para actuar sobre os variados componentes do produto. Como cada produto é elaborado com especificações próprias, o respectivo controlador obedece a parâmetros próprios. Os tipos de serviços que disponibiliza, assim como as conexões, são, na maioria dos casos, idênticos entre fabricantes. Um levantamento de todas as características dos controladores de CIB no mercado conduz à identificação de um conjunto de possibilidades de expansão do próprio controlador geral, não o limitando assim às características do próprio controlador da EFACEC.

**Tycon Electronics**

A Tycon Electronics disponibiliza um controlador para rectificadores e controladores da NE, CP e outros fabricantes denominado *Galaxy Pulsar Plus*. Este controlador suporta até 60 módulos de energia, apresentando dez tipos de alarmes com níveis de prioridade diferentes, sete dos quais configuráveis pelo utilizador.

Apresenta opções de monitorização e controlo das baterias tais como:

- Modo de controlo da temperatura através da actuação sobre a tensão;

- Controlo sobre o limite de corrente durante a recarga;

- Controlo de múltiplos contactos;

- Monitorização de valor médio de tensão;

- Monitorização da temperatura;

- Teste de descarga e previsão da carga restante nas baterias.

Figura 4 – Vista lateral da Galaxy Pulsar Plus


Figura 5 – Vista frontal da Galaxy Pulsar Plus

Em termos de monitorização e controlo, apresenta a opção de controlo local (através de um monitor de LCD e teclado embutido e de uma interface Ethernet) e controlo remoto (através de uma ligação Ethernet LAN) com três níveis de segurança distintos. É dotado de um servidor *Web* para acesso de controlo e monitorização do CIB, tanto para ligações locais como para remotas. A sua interface Ethernet suporta TCP/IP, FTP, Telnet, HTTP e SMTP. Entre as suas funcionalidades estão, para além dos 10 alarmes configuráveis e com vários níveis de prioridade, informação extensa sobre correntes, tensões e estado, suporte para conversor DC/DC, servidor DHCP, gestão avançada de baterias, histórico, estatísticas e histórico de tendências.

Em termos de conexões, apresenta duas entradas 10/100 Base-T, uma entrada DB9 para suporte a RS-232 assíncrono e uma entrada RJ11 para ligação de linha telefónica (opção modem analógico) [7].

Outro produto da Tycon Electronics é o *Galaxy Millenium*$^{TM}$ *Controller.* Este controlador permite monitorizar e controlar até 64 rectificadores, embora esteja dotado da capacidade de controlar instalações de energia, baterias de apoio, geradores de emergência, armários de fornecimento de tenção AC, *etc.*

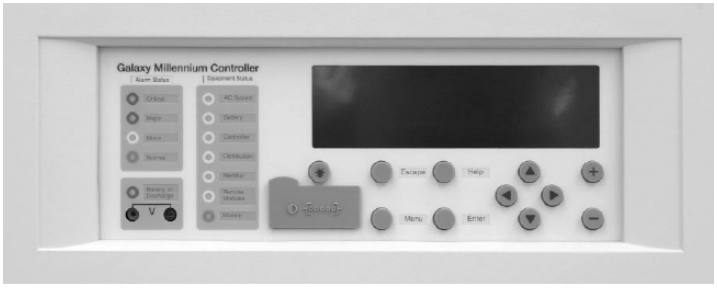


Figura 6 – Galaxy Millenium

Em termos de características, tem vários níveis de segurança, controlados por *passwords* de segurança, guarda dados de configuração básica de alarmes em memória não volátil e guarda dados de configurações de alto nível e histórico em memória RAM com suporte de uma bateria. Em termos de acesso local dispõe de um ecrã LCD e teclado embutido e, para acesso remoto, dispõe de uma interface de linha de comandos ANSI T1.317 para aceder através de um terminal de computador ou modem, *software* EasyView para ser executado em Microsoft Windows, interface TL1 e X.25 através de um terminal de PC e TCP/IP através da *Galaxy Gateway*$^{TM}$ e rede. Dispõe ainda de um conector RS-232 para acesso local e para impressão de histórico, *upgrade* de *software* (local e remoto) e acesso remoto via modem (14,4 kb/s) [8].

**UNIPOWER Telecom**

A UNIPOWER Telecom apresenta o *PCM500* como solução para monitorização e controlo de rectificadores. Consegue controlar até 16 rectificadores e é compatível com rectificadores da Mercury e Vanguard. Em termos de funcionalidades este controlador é mais básico, não possuindo qualquer *webserver* ou ligação a PC. Está

munido de DIP *Switches* que permitem activar ou desactivar rectificadores, e possui as seguintes funcionalidades:

- Protecção contra polaridade inversa;
- Tensão média ajustável;
- Possibilidade de igualar a tensão à saída de todos os rectificadores;
- Opção de compensação da temperatura na bateria;
- Amperímetro e voltímetro digital em ecrã LCD;
- 8 LED de alarme
- Alarmes de sobretensão e de subtensão;
- Pontos de teste de tensão e corrente das baterias [9];

Figura 7 – PCM 500 Series

Esta empresa, UNIPOWER Telecom**,** disponibiliza ainda outro controlador, o *Gravitas DSC1000*. Este controlador suporta até 64 rectificadores e permite controlo e monitorização local e controlo remoto. Entre as características deste dispositivo destacam-se:

- Comunicação com suporte Ethernet (RJ45);
- Conexões no protocolo $I^2C$ com os rectificadores através de ligações de linhas analógicas (RJ11);
- Envio de alarmes por *email*;
- Painel frontal ou programação baseada em *Web*;

- Display de LCD com teclado embutido;

- Compensação para temperatura da bateria;

- Opção separada para *software* SNMP [10];

- *Webserver* embutido através de TCP/IP [11];


Figura 8 – Gravitas DSC1000

**Eltek Valere**

A Eltek Valere apresenta o *Smartpack* como solução para a monitorização e controlo de CIB. Este equipamento é utilizado nos conversores do tipo *Flatpack2* e *Powerpack*. Tem como principais características:

- Painel frontal LCD e teclado;

- Interface USB ou RS-232 para monitorizar e controlar localmente ou remotamente através de SNMP, Modem, Ethernet ou servidor HTTP;

- Seis relés programáveis para controlo remoto tradicional;

- Seis entradas de dados programáveis para monitorização de outro equipamento no *site*;

- Compensação da temperatura das baterias para aumento do seu tempo de vida útil;

- Indicação da carga restante na bateria e estimativa de duração;

- Protecção por *password* para vários níveis de acesso;

- Histórico de alarmes/eventos com data;

- *Software* de comunicação baseado em Microsoft Windows [13].


Figura 9 – Eltek Smartpack

**Rectifiers Technologies**

A empresa Rectifiers Technologies apresenta um produto para a sua linha de rectificadores que é o controlador de rectificadores *MiniCSU-2*. Este rectificador está preparado para controlar até 225 rectificadores em paralelo e apresenta um painel frontal para supervisão e controlo, com teclado integrado.


Figura 10 – MiniCSU-2

As suas características incluem:

- Conexão à Ethernet via conector 10/100 Base-T;

- Interface TCP/IP;

- Vários níveis de acesso para utilizadores;

- Sistema protegido por nome de utilizador e *password*;

- Sensores de corrente, tensão e temperatura nas baterias;

- Corte de tensão automático;

- Quatro relés de alarme;

- Detecção de baixa tensão [20].

**EFACEC**

A EFACEC – Sistemas de Electrónica, S.A. apresenta como solução de controlador de CIB a gama de PSM (*MiniPSM* e *PSM*). Permite o controlo individual de até 48 rectificadores, com detecção automática de rectificadores presentes no sistema e de rectificadores avariados.


Figura 11 – PSM EFACEC

Além de funções de detecção e controlo dos CIB, oferece ainda:

- Ecrã LCD com teclado embutido;

- Interface RS-232C para ligação a PC remoto ou local;

- Duas interfaces RS-485 para ligação a redes multiponto;

- Opcionalmente, outras interfaces (RS-485, RS-422, TCP/IP);

- Porta paralela para ligação a impressora;

- Modem interno ou externo opcional;

- Estabelecimento automático de chamada para centro de comando em caso de alarme;

- *Software* de monitorização e controlo em ambiente Windows;

- Menus com protecção por *password*;

- Armazenamento de alarmes (255) em memória não volátil;

- Configuração alterável via interface RS-232C no local ou à distância [17].

### 2.5.2 Servidores de Dados

Alguns controladores de CIB têm capacidade suficiente para disponibilizar a monitorização e controlo via Internet. Estão dotados de *webservers* embutidos, suporte para configuração por Telnet, SNMP e enviam alertas por *email*. Contudo, alguns fabricantes preferem separar os componentes controlador e *webserver* em módulos separados. Dessa forma, disponibilizam componentes especialmente concebidos para fornecer o suporte de acesso ao controlador via diversos através de diferentes métodos.

Normalmente, estes dispositivos são dotados de capacidade de adaptação à infra-estrutura de rede do cliente para permitir que este se adapte às limitações da rede em vez de obrigar o cliente a criar uma nova rede para se adaptar às necessidades do módulo.

**Tycon Electronics**

O produto *Galaxy Gateway*$^{TM}$ *v3*, também da Tycon Electronics, é um módulo complementar para os controladores da empresa que lhes confere a possibilidade de serem controlados remotamente. Apresenta como características principais:

- Informação em tempo real do estado e dos alarmes dos rectificadores;

- Acesso para múltiplos utilizadores;

- Acesso global através do Internet Explorer ou Netscape Navigator;

- Não necessita de linhas dedicadas;

- Segurança reforçada e níveis múltiplos de acesso;

- Capacidade de enviar alarmes por SNMP;

- Serviço de *pager* SNMP;

- Actualização remota de *software* por FTP;

- Actualização por Telnet do *software* remoto inteligente de controlo;

- Gestão da rede através de SNMP e TL1.

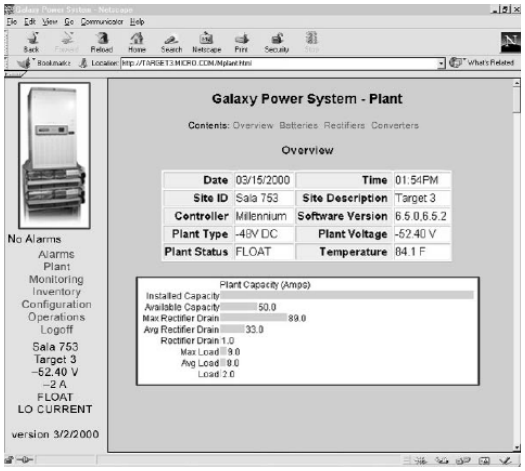


Figura 12 – Galaxy Gateway

A *Galaxy Gateway* oferece suporte para sistemas operativos *standard* de gestão de múltiplos componentes tais como o **HP OpenView – Network Node Manager** e **Lucent One Vision**. O protocolo *SNMP v2* permite enviar alarmes para os vários módulos da rede do sistema de controlo. A Galaxy Gateway comunica com cada rede através de TCP/IP. O *software* da Gateway incluí:

- *Webserver* com suporte HTTP;

- Interface via linha de comandos utilizando o Telnet;

- Um sistema de ficheiros com suporte para *upload* de ficheiros por FTP;

- *Software* cliente de gestão de redes com suporte para SNMP e TL1.

Um conector 10 Base-T (RJ-45) é utilizado para conectar o Galaxy Gateway à rede LAN/WAN. O Galaxy Gateway foi especialmente concebido para os controladores Galaxy SC, Millennium e Vector [12].

**Rectifiers Technologies**

A empresa Rectifiers Technologies apresenta um produto para a sua linha de rectificadores chamado *WebCSU* que dota o controlador de rectificadores *MiniCSU-2* da capacidade de controlo e monitorização remota. O *WebCSU* é um servidor *Web* embutido que disponibiliza serviços de HTTP e SNMP, além de comunicar com os *software*s proprietários de gestão *WinCSU*.

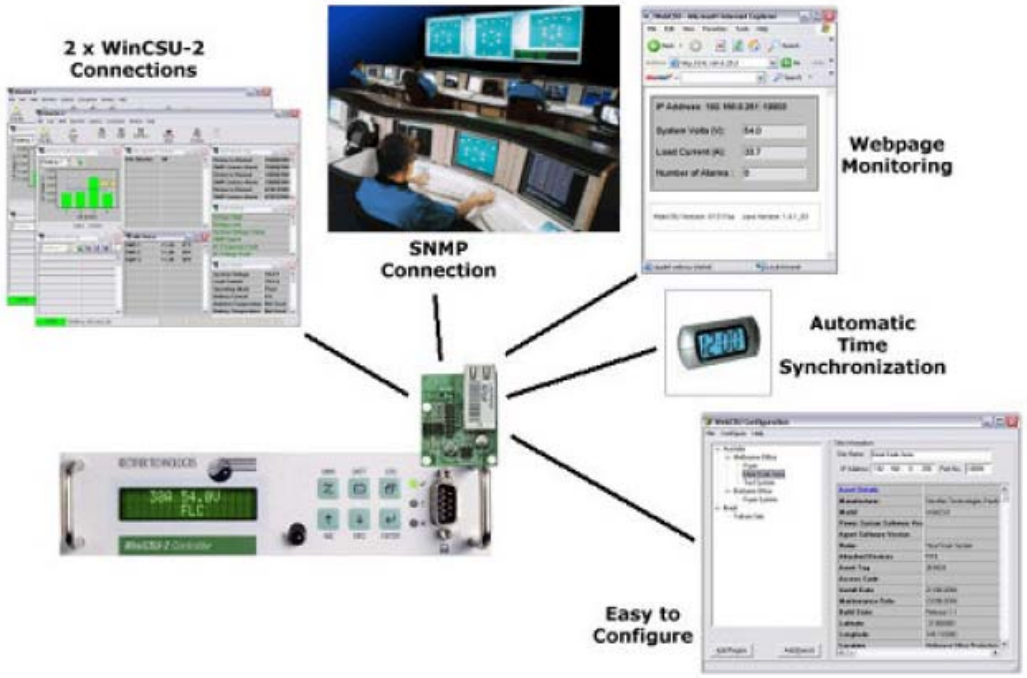


Figura 13 – Arquitectura WebCSU

Em termos de características, o *WebCSU* disponibiliza:

- Acesso à leitura de parâmetros, estados e alarmes através de SNMP;
- Sistema de *Plug N' Play* para sistema MiniCSU-2;
- Possibilidade de fazer a actualização de *firmware* remotamente;

- Ferramenta de configuração remota baseada em Windows;

- Função de cliente de SNTP para sincronizar relógio interno de MiniCSU-2;

- *Webserver* de HTTP incorporado [14].

**Generex**

A Generex disponibiliza um conjunto de servidores *Web*/SNMP da família *CS121* compatíveis com mais de 1400 UPS e geradores de energia. Apresenta como características:

- Ser um módulo de pequenas dimensões;

- Ligações via interface série;

- *Traps* de SNMP para monitorização remota e alarmes;

- Conexão Telnet;

- Histórico em tempo real;

- Conexão de rede de 10/100 Mb/s Ethernet;

- Cliente de *email* para envio de alertas de alarme;

- Servidor HTTP embutido com representação gráfica da UPS.

- SNMP.

Figura 14 – Generex CS121R

Este dispositivo apresenta visualização gráfica da UPS através da plataforma JAVAMON, não estando esta opção disponível em todos os modelos [15].

**MGE**

Outra empresa, a MGE, oferece sistemas semelhantes, tais como o *SNMP/Web Minislot Card* e o *SNMP/WEB Transverse Card*. Entre as características deste produto temos:

- Suporte para monitorização SNMP;
- *Webserver* embutido;
- 10/100 Mb/s Ethernet;
- Protocolo de segurança SSL;
- Sensor de temperatura e humidade;
- Notificações de alarme através de *email*, *pager* e SMS;

Figura 15 - SNMP/WEB Transverse Card

O serviço HTTP disponibilizado por esta *slot* SNMP permite igualmente a visualização e configuração de características da UPS a que se destina. Tem uma interface gráfica reduzida mas eficaz. Tem um registo de alarmes, visualização de parâmetros da UPS e capacidade de configuração do sistema e do próprio módulo [16].

**SENA**

A SENA oferece também soluções na área de monitorização e controlo de componentes em redes de automação. Apresentam pequenos componentes de interface de rede para converter dados de RS-232 para 10 Base-T Ethernet (RJ45) denominados *LS100*.

Figura 16 – LS100 da SENA

Estes produtos destinam-se a integrar vários tipos de componentes numa rede IP, permitindo o seu controlo e monitorização remoto. Apresentam como características :

- Suporte para Ethernet via conector RJ45;

- Suporte para 802.11b Wi-Fi;

- Suporte para protocolos ARP, IP/ICMP, TCP/IP, Telnet, DHCP *client*, PPPoE e DNS;

- Controlo através de Telnet, conexão série ou Hello Device Manager™.

Em termos de arquitectura de ligação à estrutura de comunicação, o LS100 liga-se directamente aos componentes por RS-232, permitindo o acesso remoto através de uma ligação comum via Ethernet [18].

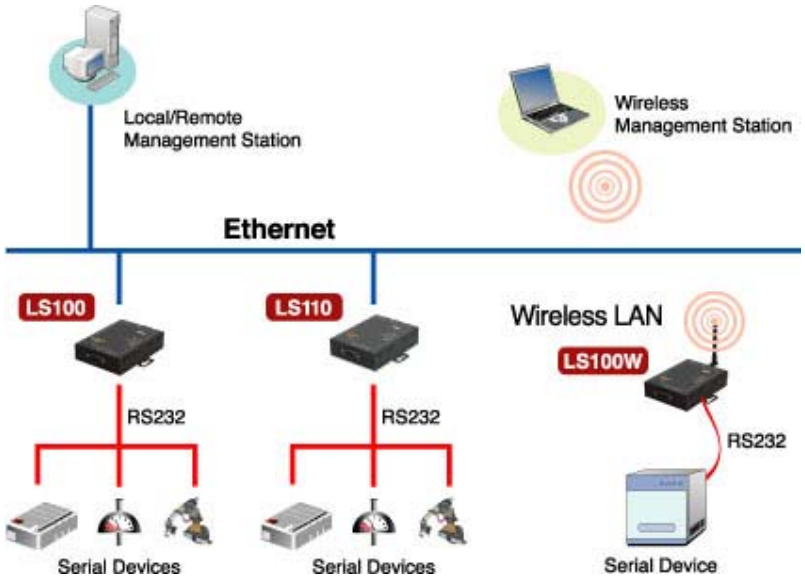


Figura 17 – Arquitectura de ligações do LS100

Outro produto da mesma empresa é o *SS100*. Este servidor de componentes recorre a uma ligação série (RS-232, RS-422, RS-485), permitindo disponibilizar essa informação para a rede IP (ligação 10/100 Base-T). Incorpora vários modos de operação tais como ligação TCP/UDP, controlo por Telnet através do porto COM e encriptação SSL.


Figura 18 – SS100 da SENA

Em termos de características, o produto apresenta:

- Conexão a rede IP 10/100 Mb/s;

- Suporta ligação série RS-232/422/485 até 230 kb/s;

- Suporte flexível para múltiplas ligações TCP/UDP para transferência de dados;

- Suporte para protocolos de segurança tais como SSL, RC4 e 3DES;

- Histórico de acessos por utilizador e por portos;

- DNS dinâmico e protocolo PPPoE para ligações DSL;

- Configuração via *Web*, Telnet/SSH ou porto série;

- *Software* de configuração e gestão.

- Protocolos suportados via interface Ethernet: ARP, IP/ICMP, DNS, SMTP com e sem autenticação, cliente DHCP, NTP, PPPoE, TCP, UDP, SSL v2 & v3, TLS v1, RFC-2217, SSH v1 & v2,Telnet, HTTP, HTTPS, SNMP v1 & v2;

- Protocolos suportados via interface série: Telnet, TCP, UDP, SSL v2 & v3, TLS v1, RFC-2217;

- Sistema Operativo Linux embebido;

- Actualização de *firmware* por FTP;

- Segurança: nome de utilizador e *password*, HTTPS, SSLv2/v3, TLS v1, 3DES e RC4, filtragem de IP, SCP.

Em termos de esquema de conexões na rede, o SS100 apresenta o seguinte aspecto [19]:

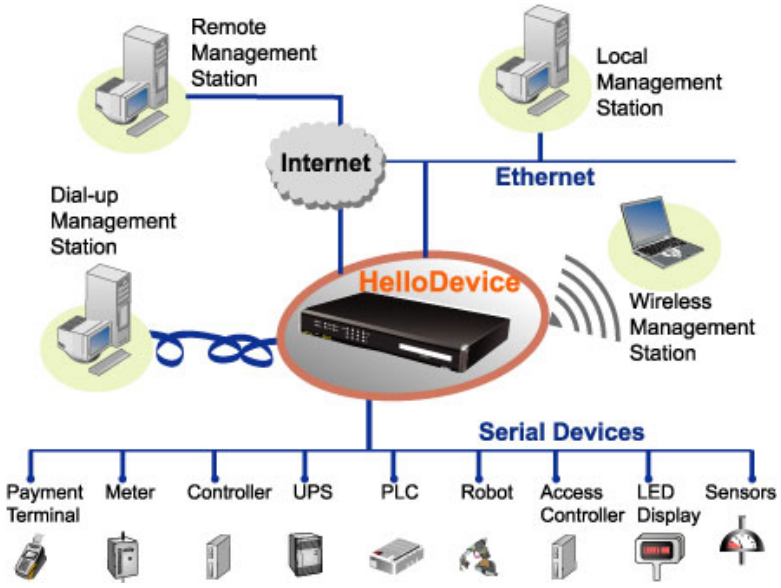


Figura 19 – Arquitectura de conexões do SS100

**EFACEC**

O complemento para o *PSM* da EFACEC é o Efapower SNMP. Este equipamento recebe dados dos PSM através da ligação RS-232C e disponibiliza monitorização e controlo remoto através de:

- Telnet via TCP/IP;

- Protocolo SNMP;

- *Webserver* embutido.

- Suporte para protocolos ARP, IP/ICMP, TCP/IP, Telnet, DHCP *client*, PPP e DNS;

- Protocolos suportados via interface Ethernet: ARP, IP/ICMP, DNS, DNS, SMTP com e sem autenticação, cliente DHCP, PPP, TCP, UDP, SSH v1 & v2, Telnet, HTTP, SNMP v1;

- Protocolos suportados via interface série: Telnet, TCP, UDP, PPP, RFC-2217;

- Sistema Operativo Linux embebido;

- Actualização de *firmware* por FTP;

- Segurança: Nome de utilizador e *password*.


Figura 20 – Efapower SNMP

Este produto apresenta suporte para HTTP, TCP/IP, Telnet, SNMP e ligação a modem analógico externo. Apresenta um sistema de autenticação por *password* com diferentes níveis de acesso [6].

**ACT'L**

A ACT'L possui na gama de produtos *eWON* um *gateway* industrial programável. Os módulos de série eWON 4001 têm como características principais interface Ethernet 10/100 Base Tx, interface série RS-485, modem PSTN, ISDN ou GSM, *router* TCP/IP + NAT, suporte para modem Modbus/TCP e Modbus/485, suporte para SNMP MIB2, um relé de saída, EMC, alimentação AC ou DC, *firewall* embebida, funções de *call-back* para redes *dial-up*, suporte dinâmico DNS, suporte par *dial-on-demand*, comunicação série e notificações de alarme por SMS, *email*, FTP e *traps* de SNMP [33].


Figura 21 – eWON 4001

## 2.6 Soluções de Fabricantes de UPS

O mercado de UPS é mais abrangente. Existem UPS de baixa potência (PC individuais), UPS de média potência (para redes de escritórios e algumas máquinas de alimentação DC de baixo consumo) e UPS de alta potência (para grandes escritórios, máquinas de elevado consumo, *etc*.).

Regra geral são as UPS de média e alta potência que permitem comunicação com um servidor. Devido à sua importância e capacidade, há interesse em monitorizar e controlar este tipo de equipamentos através de um sistema integrado. Há vários fabricantes a oferecer vários tipos de UPS, com as mais diversas características, incluído a *Efapower* da EFACEC.

**GE Digital Energy**

A GE Digital Energy, da General Electric, disponibiliza a linha de UPS *LanPro 11/31T*. Estas UPS são trifásicas, de média potência, permitindo manter uma tensão regulada e estável por um longo período de tempo. Sem entrar em especificações técnicas acerca do seu funcionamento, analisaram-se apenas as suas características de conectividade, monitorização e controlo. Esta família apresenta um LCD frontal com 6 tipos de informação relativa ao seu funcionamento: *default*, informações, *setup*, serviços, estado/alarmes, testes.

Figura 22 – LanPro 11/31T

Nas informações de ***default*** encontramos o modelo da UPS e o valor da sua carga restante. Nas **informações** encontramos temperatura, tensão de entrada, tensão de saída, frequência, carga restante (em caso de quebra de alimentação), tempo de actividade da UPS. No ***setup*** podemos obter a frequência de operação, a tensão nominal, a capacidade da bateria, a língua do dispositivo, *etc*. Nos **serviços** temos informações sobre a velocidade da ventoinha de dissipação de calor, da versão do *software*, da opção de reinício automático, *etc*. Nos **estados/alarmes** temos o histórico de eventos, tais como alarmes, falha de alimentação, erros e estados. Nos **testes** temos alguns testes disponíveis tais como o teste geral ao sistema, teste rápido de baterias e teste de calibração de baterias.

Em termos de interfaces de comunicação, o *LanPro 11/31T* dispõe de um conector DB-9 para interface RS-232 a um PC. É possível adquirir uma placa de interface Ethernet que suporta SNMP [23].

A GE Digital Energy oferece para gestão à distância de UPS, o sistema IRIS*™* - *Internet Remote Information System™*. Através deste sistema é possível efectuar a monitorização remota de UPS de forma segura.

Pode-se, também, incorporar no sistema IRIS*™,* contactos auxiliares externos à UPS, tais como *status* de operação de geradores, ar condicionado ou quaisquer outros equipamentos que estejam disponíveis no local. O sistema IRIS™ possibilita o envio automático de mensagens via *email*, *pager* ou fax para uma lista pré-definida de destinatários, possibilitando uma maior agilidade das equipas de manutenção. De

instalação simples e rápida, o sistema IRIS™ necessita somente de um módulo *InterLinc*, de um modem e de uma linha telefónica para seu funcionamento [24].

Os *softwares* de gestão prevêem acesso remoto à UPS e podem gerir várias unidades ao mesmo tempo, assegurando um eficiente controlo da qualidade de energia. Com estes programas, o responsável pela gestão da rede pode monitorizar e controlar a UPS de modo remoto ou local. Para esse propósito pode ser usada uma interface SNMP, série (RS-232) ou modem.

Figura 23 – *Software* de gestão de UPS

O PowerJUMP™ permite uma fácil integração aos vários *software*s de sistemas de gestão de rede disponíveis no mercado e pode também ser integrado ao sistema IRIS.

*Softwares* de Gestão:

- PowerJUMPin™;
- PowerJUMP Manager™;
- IRIS™ - Internet Remote Information System™;
- UPS Service tools [25].

**Salicru**

A Salicru disponibiliza a série *SLC Link* que disponibilizam uma gama de tensão que vai de 700 kVA a 10 kVA. Permite a conversão AC/DC e DC/AC, controlo digital com LCD incorporado, conexão por RS-232 e USB e comunicação por SNMP (opcional).

Figura 24 – SLC Link

**Piller Power Systems**

A Piller Power Systems disponibiliza o equipamento *UNIBLOCK*, uma UPS concebida destinada à protecção de equipamento de desenvolvimento biotecnológico, estações de difusão de rádio e televisão, instalações de saúde, processos industriais, sistemas de informação, produção farmacêutica e redes de telecomunicações. Com um Tempo Mínimo Entre Falhas (MTBF) superior a 1 200 000 h, este equipamento garante elevada fiabilidade.

Figura 25 - UNIBLOCK

Para além de um ecrã de cristais líquidos com sinóptico, o UNIBLOCK apresenta ainda as seguintes capacidades de conexão:

- Interfaces RS-232 e RS-485;
- Integração em rede SNMP via interface Ethernet;
- Protocolos MODIBUS e PROFIBUS;
- Monitorização e controlo remoto (APOCONNECT) [26].

**EFACEC**

A Efapower, da EFACEC - Sistemas de Electrónica S.A**.,** oferece a gama de UPS *MegaLine*. Esta gama de UPS disponibiliza potência dos 1250 VA até aos 10 kVA, com redundância, funcionamento do tipo *online* de dupla conversão, gestão "inteligente" de carga e descarga, mostrador alfanumérico e possibilidade de controlo remoto.

Figura 26 – UPS MegaLine

Esta linha apresenta a seguinte um conjunto de informação que se detalha na tabela seguinte.

Tabela 2 – Estados da MegaLine

| Medidas de estado da UPS no Display | |
|---|---|
| **Informação da UPS**<br>- Modelo<br>- Potência<br>- Versão de Software<br>- Nº de série da UPS<br>- Nº de módulos de potência instalados<br>- Nº de módulos de potência fora de serviço | **Informação da saída**<br>- Potência activa (W)<br>- Potência aparente (VA)<br>- Tensão de saída (V)<br>- Corrente de saída (A)<br>- Picos de corrente (A)<br>- Frequência de saída (Hz)<br>- Factor de potência da carga |
| **Informação da entrada**<br>- Potência activa (W)<br>- Potência aparente (VA)<br>- Tensão de entrada (V)<br>- Corrente de entrada (A)<br>- Picos de corrente (A)<br>- Frequência de entrada (Hz)<br>- Factor de potência na entrada | **Informação da temperatura**<br>- Temperatura interna<br>- Temperatura externa |
| **Informação das baterias**<br>- Tensão da bateria (V)<br>- Percentagem de carga<br>- Contador de intervenções de bateria<br>- nº de baterias | **Informação do histórico**<br>- Tempo de funcionamento da UPS<br>- Tempo de funcionamento da bateria<br>- Nº de shutdowns da UPS<br>- Nº de intervenções do booster<br>- Nº de intervenções do bypass<br>- Nº de registos de sobreaquecimento |

Em termos de conectividade, disponibiliza uma interface RS-232 (CCITT V28) para ligar a um PC, com a possibilidade de aceder ao histórico e parâmetros de funcionamentos da UPS. Dispõe ainda de um *software* próprio para este efeito [27].


Figura 27 – Mostrador da MegaLine

## 2.7 Protocolos de Comunicação

Após análise aos diversos sistemas, podemos sintetizar o acesso aos dados dos CIB e das UPS de duas formas distintas: via interface Ethernet e via interface série. Por exemplo, no caso dos CIB da EFACEC, se utilizarmos apenas o controlador PSM apenas teremos dados disponibilizados através da ligação série, se tivermos o módulo SNMP, teremos dados enviados por SNMP. Generalizando, temos:

Para CIB:

- Interface Ethernet: SNMP;
- Interface Série: RS-232;

Para UPS:

- Interface Ethernet: SNMP, MODBUS/TCP;
- Interface Série: RS-232, MODBUS, PROFIBUS.

Para melhor escolher os protocolos a implementar no servidor e como o fazer, será feito um estudo sobre estes protocolos.

### 2.7.1 SNMP

O protocolo *Simple Network Management Protocol* (SNMP) – é um protocolo de gestão típica de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede como placas e comutadores (*switches*). O

SNMP possibilita aos administradores de rede gerir o desempenho da rede, encontrar e resolver seus eventuais problemas, e, entre outras opções, fornecer dados para o planeamento de sua expansão.

O *software* de gestão de redes segue o modelo cliente-servidor convencional: uma aplicação 'servidora' na máquina cliente e uma aplicação 'cliente' no dispositivo de rede a ser analisado ou monitorizado. Para evitar confusão com outras aplicações de rede, os sistemas de gestão de redes evitam os termos “cliente” e “servidor” e optam por usar “gestor” para a aplicação servidora e “agente” para a aplicação cliente que roda no dispositivo de rede.

Uma rede gerida pelo protocolo SNMP é formada por quatro componentes chaves:

- Dispositivos Geridos;
- Placas de rede;
- Agentes;
- Sistemas de Gestão de Redes – *Network-Management Systems* (NMS).

Um Dispositivo Gerido é um nó de rede que possui um agente SNMP instalado e se encontra numa rede gerida. Estes dispositivos colectam e armazenam informações de gestão e mantém estas informações disponíveis para sistemas NMS através do protocolo SNMP. Os dispositivos geridos, também às vezes denominados dispositivos de rede, podem ser *routers*, servidores de acesso, impressoras, computadores, servidores de rede, *switches*, dispositivos de armazenamento, *etc.*.

Um Agente é um módulo de *software* de gestão de rede que fica armazenado num Dispositivo Gerido. Um agente tem o conhecimento das informações de gestão locais e traduz estas informações para um formato compatível com o protocolo SNMP.

Um sistema NMS é responsável pelas aplicações que monitorizam e controlam os Dispositivos Geridos. Normalmente, é instalado num (ou mais de um) servidor de

rede dedicado a estas operações de gestão, que recebe informações (pacotes SNMP) de todos os Dispositivos Geridos daquela rede.

O SNMP v1 é um protocolo padrão usado para gestão de redes que define os formatos dos pedidos que o Gestor envia para o Agente e os formatos das respostas que o agente retorna, assim como o significado exacto de cada pedido e resposta. Uma mensagem SNMP é codificada com um padrão designado de ASN.1 (*Abstract Syntax Notation.1*).

Para permitir a transferência de grandes inteiros, sem desperdiçar espaço em cada transferência, o ASN.1 usa uma combinação do tamanho e valor de cada objecto a ser transferido. O SNMP não define um grande número de comandos. Em lugar disso, define duas operações básicas:

- *fetch*, para obter um valor de um dispositivo;

- *store*, para colocar um valor num dispositivo.

O comando que especifica uma operação de *fetch* ou *store* deve especificar o nome do objecto, que é único.

Suponhamos o caso de um contador de erros de CRC – *Cyclic Redundancy Check.* Uma vez que o SNMP não inclui comandos específicos para fazer *reset* do contador, uma forma simples é colocar zero no contador. Neste caso, o Gestor faz o *fetch* (leitura) do parâmetro desejado para determinar o estado do dispositivo. As operações que controlam o dispositivo são definidas como efeitos secundários de *store* (alterar/gravar valores) em objectos.

O SNMP especifica (na versão 1) quatro unidades de dados do protocolo (PDU):

- GET, usado para retirar um pedaço de informação de gestão.

- GETNEXT, usado interactivamente para retirar sequências de informação de gestão.

- SET, usado para fazer uma mudança no subsistema gerido.

- TRAP, usado para reportar uma notificação ou para outros eventos assíncronos sobre o subsistema gerido.

- Todos os objectos acedidos pelo SNMP devem ter nomes únicos definidos e atribuídos. Além disso, o *Gestor* e o *Agente* devem acordar os nomes e significados das operações *fetch* e *store*. O conjunto de todos os objectos SNMP é colectivamente conhecido como MIB (*Management Information Base*). O *standard* SNMP não define a MIB, mas apenas o formato e o tipo de codificação das mensagens. A especificação das variáveis MIB, assim como o significado das operações *fetch* e *store* em cada variável, são especificados por um padrão próprio.

A definição dos objectos da MIB é feita com o esquema de nomes do ASN.1, o qual atribui a cada objecto um prefixo longo que garante a unicidade do nome (a cada nome é atribuído um número inteiro). O SNMP não especifica conjuntos de variáveis e a definição de objectos é independente do protocolo de comunicação, permitindo criar novos conjuntos de variáveis MIB, definidos como *standards*, para novos dispositivos ou novos protocolos. Por esta razão, foram criados muitos conjuntos de variáveis MIB que correspondem a protocolos como UDP, IP ou ARP, assim como variáveis MIB para *hardware* de rede como Ethernet, FDDI ou para dispositivos tais como *bridges*, *switches* ou impressoras [30].

### 2.7.2 Comunicação Série por RS-232

A comunicação por RS-232, também conhecida por EIA RS-232C ou V.24, é um padrão bastante antigo mas que continua a ser utilizada devido à sua simplicidade e confiabilidade. Como em qualquer dispositivo de transmissão série, os bits são enviados um a um, sequencialmente, e, normalmente, com o bit menos significativo em primeiro lugar (*LSB*). Como se trata de protocolo assíncrono, *i.e.*, sem sincronismo de relógio (*clock*), é da responsabilidade do transmissor e do receptor efectuarem os controlos de tempo para saber quando cada bit começa e acaba.

Na sua forma padrão, o RS-232 utiliza dois sinais de controlo, o RTS (*ready to send*) e o CTS (*clear to send*) para efectuar o controlo de fluxo via *hardware*. Basicamente, quando o transmissor deseja começar uma transmissão sinaliza

através do pino RTS. O receptor, ao perceber que o transmissor deseja enviar algum dado, prepara-se para recebê-lo e activa o pino CTS. Apenas depois de receber o sinal CTS, o transmissor pode começar a transmissão.

Para cada byte enviado existem bits de *start* e *stop*; o mais comum é utilizar-se um bit de início (*start* bit) e um bit de finalização (*stop* bit), mas é possível encontrar aplicações que utilizam um bit e meio (1,5 b) ou dois bits (2 b) de início/finalização. A figura abaixo mostra como a transmissão de um byte ocorre:

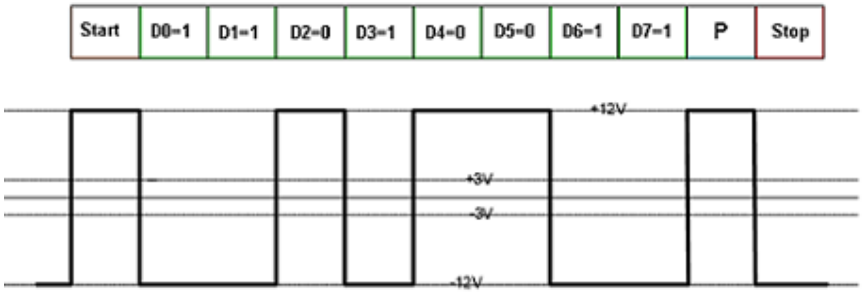


Figura 28 – Transmissão RS-232

Como já foi citado anteriormente, esta transmissão é assíncrona. Tendo a velocidade de comunicação sido ajustada nos dois dispositivos inicialmente, cada um sabe quanto tempo demora um bit para ser transmitido, e é com base nesta informação que a identificação dos bits é possível.

Do lado do transmissor, o envio resume-se basicamente a enviar um bit de início, aguardar um período de tempo, e enviar os próximos 8 b mais 1 b de *stop bit*, com o mesmo intervalo de tempo entre eles. No receptor, após a primeira descida de nível lógico (nível lógico de "1" para "0") (*start* bit) o receptor sabe que uma sequência de mais 8 b de dados mais 1 b de *stop* chegará. Dado que se conhece a velocidade de transmissão, então tudo que se precisa de fazer é aguardar o tempo de transmissão entre cada bit e efectuar a leitura. Após receber o *stop* bit, a recepção encerra-se e o receptor volta a aguardar o próximo *start* bit.

Nos microcontroladores modernos todo este trabalho é normalmente efectuado por uma UART (*Universal Asynchronous Receiver Transmitter*). Este periférico encarrega-se de efectuar todo o controlo e apenas gerar interrupções

quando um byte é recebido. No entanto, algumas vezes o microcontrolador utilizado não possui uma UART, ou possui mas ela não está disponível. Nestes casos é possível implementar uma interface série através de *software*, implementando-se a sequência de transmissão e recepção descrita anteriormente [29].

### 2.7.3 MODBUS

O Modbus é um protocolo de comunicação de dados utilizado em sistemas de automação industrial que foi criado na década de 1970 pela Modicon. É um dos mais antigos protocolos utilizados em redes de controladores lógicos programáveis (PLC) para aquisição de sinais de instrumentos e comando de actuadores. A Modicon (actualmente parte do grupo Schneider Electric) colocou as especificações e normas que definem o Modbus no domínio público. Por esta razão, é hoje um protocolo utilizado em milhares de equipamentos existentes e é uma das soluções de rede mais baratas em automação industrial.

O Modbus utiliza o RS-232, RS-485 ou Ethernet como meio físico. O mecanismo de controlo de acesso é do tipo mestre-escravo (*master-slave*). A estação mestre (geralmente um PLC) envia mensagens solicitando dos escravos que enviem os dados lidos pela instrumentação ou envia sinais a serem escritos nas saídas para o controlo dos actuadores. O protocolo possui comandos para envio de dados discretos (entradas e saídas digitais) ou numéricos (entradas e saídas analógicas).

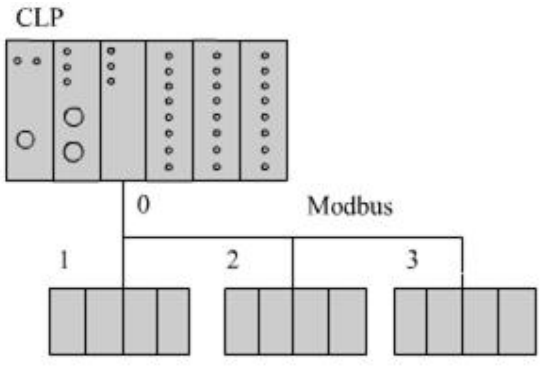


Figura 29 – Rede Modbus

A imagem acima mostra um exemplo de rede Modbus com um mestre (PLC) e três escravos (módulos de entradas e saídas, ou simplesmente E/S). Em cada ciclo de

comunicação, o PLC lê e escreve valores em cada um dos escravos. Como o sistema de controlo de acesso é do tipo mestre-escravo, nenhum dos módulos escravos inicia comunicação a não ser para responder às solicitações do mestre.

Basicamente, uma comunicação em Modbus obedece a um *frame* que contém o endereço do escravo, o comando a ser executado, uma quantidade variável de dados complementares e uma verificação de consistência de dados (CRC).

Em redes série, baseadas em RS-485 ou RS-232, o Modbus pode ter duas variações: RTU e ASCII.

**Modbus RTU**

Em Modbus RTU os dados são transmitidos em formato binário de 8 b, permitindo a compactação dos dados em pequenos pacotes. No modo RTU, os endereços e valores podem ser representados em formato binário. Números inteiros variando entre -32768 e 32767 podem ser representados por 2 B. O mesmo número precisaria de quatro caracteres ASCII para ser representado (em hexadecimal).

**Modbus ASCII**

Transmite os dados codificados em caracteres ASCII de 7 b. Apesar de gerar mensagens legíveis por pessoas este modo consome mais recursos da rede.

**Modbus/TCP**

Aqui os dados são encapsulados em formato binário em *frames* TCP para a utilização do meio físico Ethernet (IEEE 802.3). Quando o Modbus/TCP é utilizado, o mecanismo de controlo de acesso é o CSMA-CD (próprio da rede IP) e as estações utilizam o modelo cliente-servidor.

**Modbus Plus**

Esta versão que possui vários recursos adicionais de encaminhamento, diagnóstico, endereçamento e consistência de dados. O Modbus Plus é ainda mantido sob

domínio da *Schneider Electric* e só pode ser implantada sob licença deste fabricante [31].

### 2.7.4 PROFIBUS

PROFIBUS (*Process Field Bus*) é o tipo mais popular sistema de comunicação em redes Fieldbus que, em 2004, se estimava que existiriam mais de 10 milhões de nós instalados mundialmente.

O PROFIBUS foi desenvolvido em 1987 como resultado de um projecto de pesquisa alemão envolvendo 21 empresas e institutos de investigação. Na Europa, as redes PROFIBUS dominam mais de 60 % do mercado de automação industrial.

Existem três diferentes versões de PROFIBUS:

- PROFIBUS-FMS (*Fieldbus Message Specification*):
- PROFIBUS-DP (*Decentralised Periphery*);
- PROFIBUS-PA (*Process Automation*)

O PROFIBUS foi definido em 1991/1993 na norma DIN 19245, movida em 1996 para a EN 50170 e, desde 1999, incluída na norma IEC 61158/IEC 61784.

O padrão PROFIBUS é mantido, actualizado e comercializado pela PROFIBUS International, uma organização sem fins lucrativos administrada a partir de Karlsruhe na Alemanha [32].

## 2.8 *Software* de Gestão de Redes Distribuídas

No âmbito do estudo desenvolvido foi efectuado um levantamento dos *software*s de gestão existentes no mercado actual, sejam eles *open source* ou não. Desta forma, será possível comparar quais as principais diferenças entre eles, principais pontos fortes e tecnologias utilizadas. Segue-se uma lista extensa e completa (até à data) de todos os sistemas de gestão de redes (*Network Management Systems*). Desta lista serão analisados os *software*s mais utilizados e importantes [37]:

- Alcatel 5620 Network Manager & Service Aware Manager;
- Attachmate NetIQ AppManager & SecurityManager;
- Blue Coat Proxy Servers for WAN Optimization and Web cache;
- CA Unicenter Network and Systems Management;
- CA Spectrum;
- Cacti;
- Cisco Active Network Abstraction;
- CiscoWorks Lan Management Solution Manages enterprise switching networks;
- Cisco Network Analysis Module Analyzes live network traffic;
- Comarch OSS Suite;
- Crannog *Software*;
- ECI Telecom LightSoft® Multidimensional Network Management System;
- Ericsson OSSRC - Operations Support System, Radio and Core;
- Sphere Networks Network Management System;
- Hewlett Packard OpenView Framework;
- Hyperic;
- IBM AURORA Network Performance Profiling System;
- IBM Tivoli NetView;
- Intellipool Network Monitor;
- Lucent VitalSuite Network and Service Management Software;

- Lucent Navis® Optical Management System (OMS);
- Microsoft Operations Manager (MOM);
- MRTG;
- Nagios;
- Netdisco;
- NetQoS;
- NetFlow Monitor;
- Nortel Enterprise Network and Service Management;
- Nortel Enterprise Policy Manager;
- Nortel Enterprise Switch Manager;
- Nortel Proactive Voice Quality Management;
- Network Administration Visualized (NAV);
- ODCNMS;
- OmniCenter;
- OpenNMS;
- Opsware Network Automation System (NAS);
- PRTG Traffic Grapher;
- ProCurve Manager (PCM+) Comprehensive Management Software;
- Raritan Computer's CommandCenter NOC;
- ServersCheck Monitoring Software;
- Siemens Integrated Network Management Services / System;

- SolarWinds;

- TTI Telecom Service Assurance;

- DNA (Dynamic Network Abstraction);

- ZABBIX;

- Zenoss.

### 2.8.1 HP Open View

O HP Open View consistia numa gama de soluções de *software* para gestão de redes e sistemas da Hewlett Packard. Em 2007, todo o *portfolio* de *software* foi reestruturado pela divisão de *software* da HP. O HP Open View consiste actualmente num conjunto de aplicações especialmente desenhadas para controlo e monitorização de sistemas empresariais de TI (*Tecnologias de Informação*). São um conjunto de aplicações com diferentes módulos dedicados a cada tecnologia de comunicação e a cada tipo de arquitectura de rede [34].

Os produtos disponíveis nesta gama de *software* são:

- HP OpenView Network Node Manager (OV NNM);

- HP OpenView Operations (OVO) — sistemas de monitorização e aplicações que utilizam agentes:

    - para Windows (OVOW);

    - para Unix 8.1 (OVOU);

- HP OpenView ServiceCenter;

- HP OpenView AssetCenter;

- HP OpenView Service Desk (OVSD);

- HP OpenView Internet Services (OVIS);

- HP OpenView Service Navigator ;
- HP OpenView Transaction Analyzer (OVTA);
- HP OpenView SOA Manager;
- HP OpenView Reporter OpenView Reporter;

**Desempenho**

- HP OpenView Performance Agent (OVPA);
- HP OpenView Performance Insight (OVPI);
- HP OpenView Performance Manager (OVPM);
- HP OpenView Reporter (OVR);
- HP OpenView GlancePlus;

**Armazenamento**

- HP OpenView Storage Area Manager (OV SAM);
- HP OpenView Storage Data Protector;
- HP OpenView Storage Mirroring;
- HP OpenView Storage Mirroring Exchange Failover Utility;
- HP OpenView Dashboard — fornece um portal *Web* para os produtos de gestão Open View;
- HP OpenView TeMIP ;
- HP OpenView Service Activator (OVSA);
- HP OpenView Select Access — Acesso seguro e estável a informação crítica;

- HP OpenView Select Identity (OVSI) — Gestão centralizada dos recursos e permissões dos utilizadores ao longo do seu ciclo de vida ;

**HP OpenView Smart Plug-ins (SPI)**

- HP OpenView SPI para BEA Tuxedo;
- HP OpenView SPI para BEA WebLogic;
- HP OpenView SPI para BEA WebLogic Integration;
- HP OpenView SPI para Citrix;
- HP OpenView SPI para Databases (Oracle, Microsoft SQL Server, Sybase, and Informix);
- HP OpenView SPI para Documentum;
- HP OpenView SPI para IBM DB2;
- HP OpenView SPI para IBM WebSphere Application Server;
- HP OpenView SPI para Microsoft Exchange;
- HP OpenView SPI para Microsoft Windows;
- HP OpenView SPI para OpenVMS ;
- HP OpenView SPI para Oracle Application Server;
- HP OpenView SPI para PeopleSoft;
- HP OpenView SPI para Remedy ARS Integration;
- HP OpenView SPI para SAP;
- HP OpenView SPI para Siebel;
- HP OpenView SPI para Storage Area Manager;

- HP OpenView SPI para Terminal Server;
- HP OpenView SPI para TIBCO;
- HP OpenView SPI para UNIX OS;
- HP OpenView SPI para Web Servers;

**Network Node Manager SPI**

- Network Node Manager SPI para Advanced Routing;
- Network Node Manager SPI para IP Telephony;
- Network Node Manager SPI para LAN/WAN Edge;
- Network Node Manager SPI para MPLS VPN;
- Network Node Manager SPI para IP Multicast;

**HP OpenView Configuration Management**

- HP OpenView Configuration Management Application Self-Service Manager
- HP OpenView Configuration Management Application Manager
- HP OpenView Configuration Management Inventory Manager
- HP OpenView Configuration Management OS Manager
- HP OpenView Configuration Management Patch Manager
- HP OpenView Configuration Management Application Usage Manager
- HP OpenView Client Configuration Manager

Deste conjunto de módulos de *software*, é interessante analisar o HP Network Node Manager (NNM). O Network Node Manager utiliza o protocolo SNMP para comunicar com outros dispositivos na rede, permitindo-lhes serem auto-descobertos, monitorizados e controlados. O NNM determina e disponibiliza

informação graficamente acerca das ligações físicas e lógicas do sistema de comunicação assim como informação acerca dos diferentes protocolos a correr na rede. Permite ainda que o histórico da informação sobre as diferentes máquinas possa visto e analisado graficamente [35].

A versão 8.0 do NNM permite controlo até 15 000 nós, com até 50 000 *polled* interfaces e 40 utilizadores concorrentes. Para tal necessita de estar instalado num sistema com 8 CPU ou 4 processadores Dual Core de 64 b com mais de 1 GHz de velocidade de processamento cada um, um mínimo de 16 GB de RAM, 8 GB de Java *heap*, 5 GB de espaço para a instalação do sistema e 60 GB de ROM para dados durante a execução do programa.

Pode ser instalado em Windows e HP-UX e suporta um grande número de protocolos e modelos de MIB de vários fabricantes. É compatível com um grande número de equipamentos de rede de vários fabricantes tais como *switches*, *routers* e *hubs* [36].

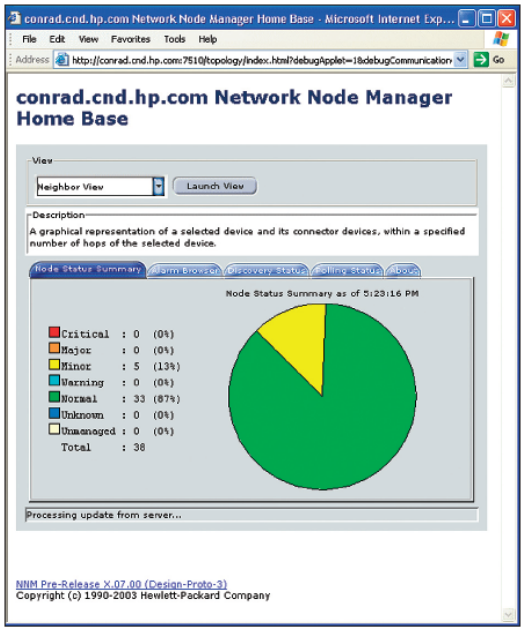


Figura 30 – Aspecto do serviço disponibilizado pelo navegador *Web*

O *software* suporta diferentes utilizadores, divididos em diferentes grupos com níveis de acesso diferenciados. A consola e controlo são disponibilizados através de um *webserver* que comunica com os navegadores *Web* do cliente através do

protocolo HTTP. O *webserver* implementado na ferramenta utiliza protocolos de segurança SSL. Utiliza o servidor de aplicações *Tomcat* da Apache para disponibilizar um serviço de HTTPS e executar aplicações *Web* baseadas em Java.

A versão do JBoss que vem com o NNM 8.0 disponibiliza o servidor Tomcat 6.0 e permite a configuração dos parâmetros da conexão entre o *webserver* e o navegador *Web* através de um ficheiro XML.

O NNM mantém-se a par do estado e dos dados dos componentes de uma rede através de uma contínua acção de levantamento do estado dos *routers* e *switches*, que são os elementos mais críticos de uma rede de interligação das diferentes máquinas. Este sistema evita que se diagnostique constantemente o estado dos elementos finais de uma rede (no caso de uma rede de escritório, PC e impressoras), sobrecarregando assim o tráfego na rede e a máquina em que corre o NNM. O número de máquinas licenciadas para o *software* Open View limitam a operacionalidade do *software* ao nível da gestão de dispositivos.

É possível fazer uma busca selectiva, através da definição da *Seed* (Semente) que se deseja procurar ou adicionar à rede. Os métodos de detecção de cada máquina da rede podem passar por uma procura da máquina pelo seu respectivo IP ou através da MIB (protocolo SNMP). Estas duas soluções são necessárias devido ao problema de não haver garantia que as máquinas tenham uma MIB compatível com as definições do NNM ou até que tenham o protocolo SNMP configurado.

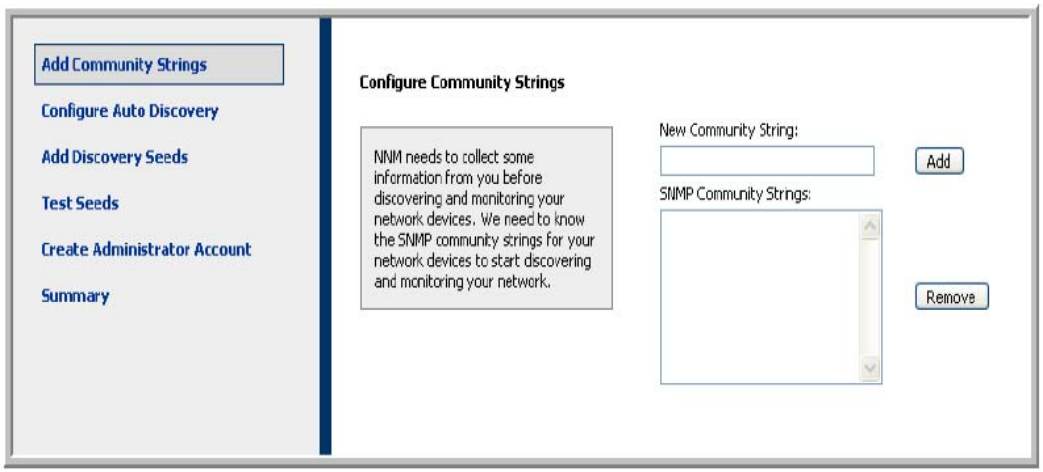


Figura 31 – Página de Configuração de Community Strings

O NNM monitoriza a rede de duas maneiras diferentes: através do *polling* de estado ou da recepção de um *trap* (alarme de incidente):

***State Polling***

O NNM envia os pedidos de estado de cada equipamento através de SNMP ou ICMP. Os pedidos de SNMP verificam se cada agente de SNMP está a responder aos pedidos de *poll*. O SNMP também envia pedidos específicos de valores da MIB de cada um dos componentes da rede: as variáveis *ifAdminStatus* e *ifOperStatus*.

O ICMP utiliza *polling* através de *ping* para os IP das máquinas para determinar se as máquinas estão acessíveis ou não. Os tempos de *polling* podem ser definidos por grupo de máquinas de forma a estabelecer períodos de interrogação diferentes para cada equipamento.

Um factor de segurança para estes sistemas é o *backup* semanal realizado pelo sistema gerido pelo NNM (informações sobre a rede e seus componentes). Estes *backups* são recomendados numa base semanal pela HP e não é necessário desactivar o NNM para os efectuar.

Estes *backups* de informação são necessários para manter uma última configuração funcional da rede no caso de esta falhar. A HP disponibiliza *scripts* para efectuar o *backup* das MIB e da restante informação de rede e *scripts* para restaurar a definição funcional.

Os dados guardados são:

- Ficheiros de configuração e respectivos directórios;

- Configurações da base de dados;

- Base de dados de topologias da rede;

- Base de dados de eventos.

Podem-se definir parâmetros, limites e restrições às contas de cada tipo de grupo e utilizador, alterando as definições de origem [37].

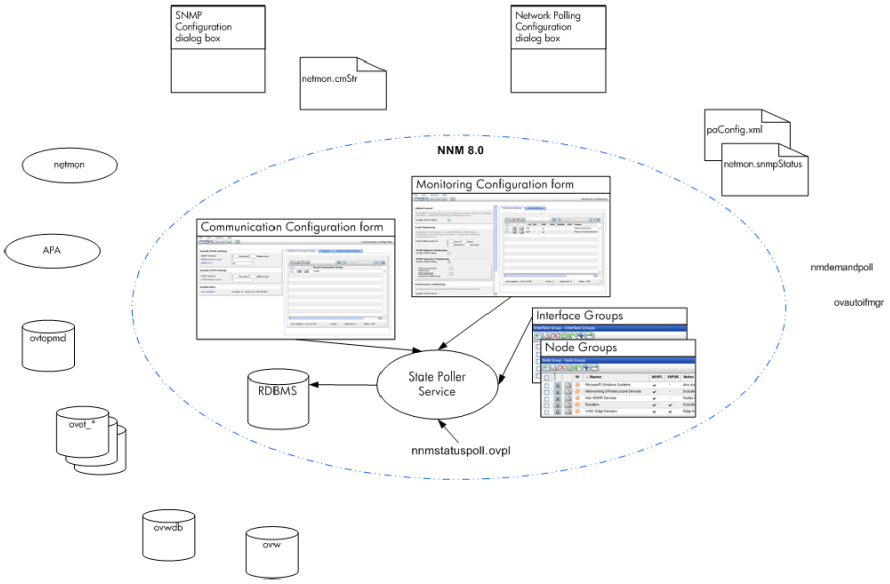


Figura 32 – Elementos de Monitorização e Configuração

### 2.8.2 Tivoli

O IBM Tivoli Management é outra ferramenta utilizada na gestão e monitorização de redes. Tal como o *software* da HP, este também foi desenvolvido para controlo de uma rede com um elevado número destes dispositivos. Da gama de produtos da divisão de *software* da IBM destacam-se [39]:

- IBM/Tivoli Distributed Monitoring Classic (DM);

- IBM/Tivoli Enterprise Console (TEC);

- IBM/Tivoli Configuration Manager;

- IBM/Tivoli Remote Control;

- IBM Tivoli NetView;

- IBM Tivoli Monitoring;

- IBM Tivoli Business Systems Manager;

- IBM Tivoli Application Dependency Discovery Manager (TADDM);

**Tivoli Common Agent Services**

O Tivoli Common Agent Services é instalado nas máquinas envolvidas e desempenha as funções de cliente do sistema de monitorização e gestão, compatibilizando as máquinas com os vários *softwares* existentes no mercado. Estes agentes recolhem informação dos recursos que gerem, disponibilizando-a para o serviço de controlo e monitorização.

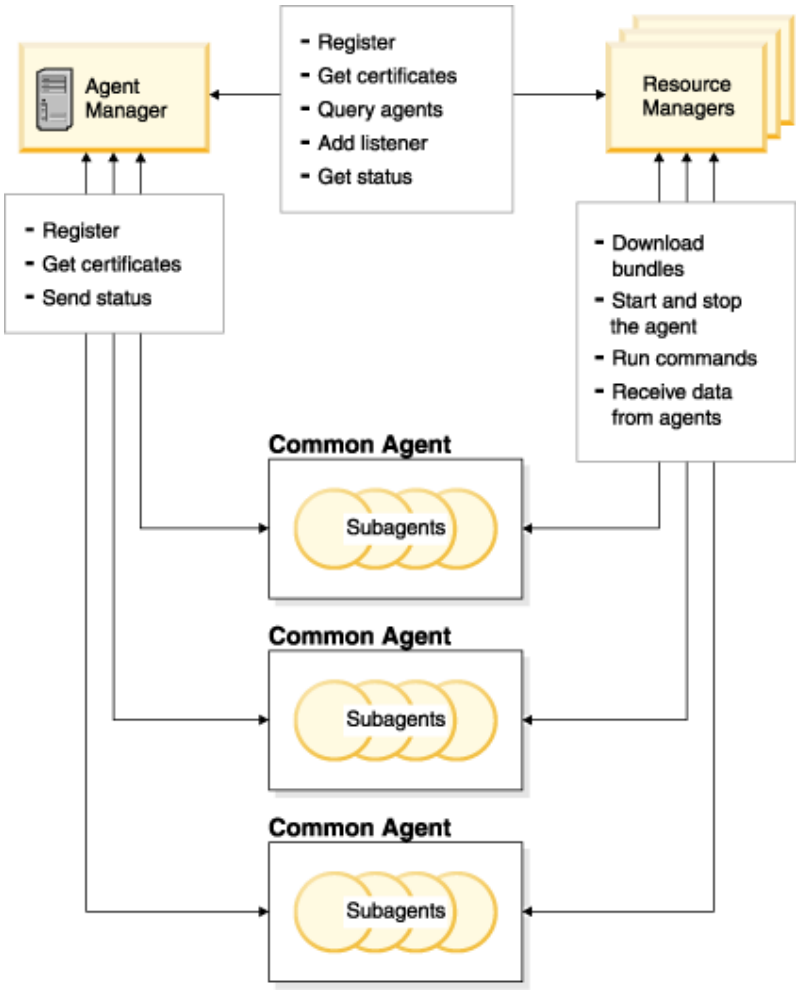


Figura 33 – Hierarquia do Tivoli Common Agent Services

O Tivoli Common Agent Services consiste nos seguintes componentes:

*Agente Comum*

O agente comum é uma entidade comum a todos os recursos. Permite que múltiplas aplicações de gestão partilharem recursos quando gerem um sistema.

*Gestor de Agente*

É o componente servidor do sistema Tivoli Common Agent Services que fornece as funcionalidades que permitem aos clientes obter informação sobre outros agentes e recursos geridos. Permite ligações seguras entre *endpoints* (equipamentos terminais), e mantém a base de dados dos gestores de recursos. Também inclui o registo de serviços, certificados de segurança, registo de acesso, encaminhamento de agentes comuns, gestão de recursos e recolha de estado.

*Gestor de Recursos*

Cada produto que utilize o Tivoli Common Agent Services tem o seu próprio gestor de recursos e subagente.

O agente comum contacta o gestor de agentes e devolve o seu estado se alguma das configurações se alterar durante os seguintes processos:

- Quando um agente comum inicia ou termina o funcionamento;
- Sempre que algo for instalado, renovado ou removido;
- Depois de um determinado período de tempo (configurável).

As interacções típicas são:

- O gestor de recursos interage com o gestor de agentes quando:
  - Se regista com o gestor de agentes;
  - Questiona a um agente comum quem está presente na rede;
  - Pede por um certificado inicial de segurança;
  - Entrega notificações de registo e configuração de agente comum.
- O gestor de recursos interage com o agente comum quando:

- Pára ou inicia os seus subagentes;
- Questiona a configuração dos agentes comuns instalados.

***Agente Comum***

O agente comum fornece:

- Operação contínua - sempre que um agente comum pára, existe um *watchdog* que o reinicia. Desta forma, garante-se que o agente comum e os subagentes estão sempre disponíveis;
- Um conjunto de credenciais de segurança e uma infra-estrutura de segurança para todas as aplicações de gestão;
- Gestão autónoma das credenciais de segurança. Sempre que um certificado de segurança de um agente se aproxima da sua data de expiração, é automaticamente renovada;
- Atribuição e gestão dos ciclos de vida dos subagentes;
- Monitorização do estado e configuração dos agentes comuns.

Os agentes comuns permitem a qualquer subagente participar e enviar informação de estado. As aplicações de gestão podem-se configurar para receber estas actualizações. Um agente comum contacta um gestor de agentes sempre que:

- Um agente comum inicia ou termina o funcionamento;
- Após um período configurável.

***Gestor de Agentes***

O gestor de agentes suporta as seguintes aplicações:

- *WebSphere Application Server*

Os produtos da família WebSphere Application Server providenciam um ambiente de aplicações muito fiável, escalar e com grande disponibilidade. É possível utilizar qualquer *software* de gestão com a aplicação WebSphere, desde um servidor simples de aplicações WebSphere até configurações mais avançadas, utilizando em servidor de *clusters*.

- *Lightweight Runtime*

O Lightweight Runtime fornece uma arquitectura para execução do gestor de agente baseada em *standards* e com pouco *overhead* de informação. O Lightweight Runtime implementa uma Framework OSGi utilizando tecnologia Eclipse.

O gestor de agente é composto pelas seguintes componentes:

- Servidor de gestor de agente;
- Registo;
- Serviço de recuperação de agente.

*Servidor de Gestor de Agente*

O servidor de gestor de servidor é um sistema informático onde o serviço de gestão de agentes e o serviço de recuperação de agentes é executado. O gestor de agentes pode ser executado sobre uma das seguintes plataformas:

- WebSphere Application Server;
- Lightweight Runtime.

Os gestores de recursos e agentes devem estar registados no gestor de agentes de modo a poderem comunicar entre si. O registo recorre a um serviço de encriptação de *password,* que separa *password* para registo de agentes de *passwords* para controlo de aplicações. Esta tipologia torna mais difícil a *trojans* ou outro tipo de aplicações registarem-se e obterem uma identificação válida.

*Registo*

O registo é uma base de dados que contém a configuração actual de todos os agentes conhecidos e gestores de recursos. O registo contém a identidade, certificados e parâmetros de comunicação de cada agente gestor de recursos e, em relação aos agentes comuns, a seguinte informação:

- A identidade de cada agente conhecido e o seu sistema de computador;
- O certificado passado a cada agente;
- Informação sobre configuração básica acerca de cada agente, incluído informação sobre o tipo e versão de *hardware* e sistema operativo;
- A configuração de cada agente (actualizada pelo agente a cada intervalo de tempo configurável);
- Os erros reportados por cada agente (actualizado pelo agente através de um intervalo configurável);
- Parâmetros actuais de comunicação para o agente, incluindo o endereço de IP, porto ou portos onde se encontra o agente e o protocolo suportado;

A informação no registo é actualizada a cada ocorrência de um evento assíncrono, tal como o registo de um agente e gestor de recursos ou uma actualização de um agente.

*Serviço de Recuperação do Agente*

O serviço de recuperação de agente é um serviço de rede que providencia um histórico de erros para agentes que não possam comunicar com outro serviço de gestor de rede. Os agentes comuns utilizam um ligação não segura (não SSL encriptada), HTTP para comunicar com o serviço de recuperação de agente, que é executado no gestor de agentes como um *servlet* da WebSphere. Devido ao facto de a ligação não ser segura, um agente pode sempre comunicar com o serviço de

recuperação de agentes, mesmo que o agente esteja incorrectamente configurado ou os certificados tenham expirado [40].

### 2.8.3 siNMS

O Integrated Network Management Services da Siemens (siNMs) é um sistema abrangente de gestão de rede. Foi inicialmente criado para ser um servidor de linguagens heterogéneas e redes de dados. Permite o aceso a sistemas individuais de gestão de redes, ou seja, directamente sobre os componentes da rede. Esta característica é particularmente importante para fornecer uma representação uniforme do estado geral da rede. É aplicado, principalmente, ao controlo de todo o tipo de sistemas que sejam capazes de enviar sinais eléctricos.

O siNMS oferece as seguintes características:

- Gestão de múltiplas tecnologias de rede tais como SDH e PDH, DWDM, GSM/UMTS, GSM-R, CaTV, ATM, IP, Acess, Enterprice, *etc*.;

- Integração de uma grande diversidade de produtos via um conceito de integração flexível, tais como Surpass, Walkair (PMP), EWSD, EWSP, HICOM, HiPath, *etc*.;

- Salvaguarda de protocolos de serviço a vários níveis;

- Serviço de gestão flexível que pode ser optimizado para adaptação ao conceito de operador de rede;

- Serviço de restauração via *prompt* em caso de detecção de erro [41].

### 2.8.4 Nagios

**Nagios** é uma popular aplicação de monitorização de rede do tipo código aberto e licenciado pelo sistema GPL – *General Public License*. Pode monitorar tanto *hosts* quanto serviços, alertando o administrador quando ocorrem problemas e também quando os problemas são resolvidos.

O Nagios foi originalmente criado sob o nome de Netsaint. Foi desenvolvido e é actualmente mantido por Ethan Galstad, com ajuda de um exército de programadores que activamente mantêm *plug-ins* oficiais e não oficiais.

Este sistema foi originalmente concebido para o sistema operacional Linux, mas executa igualmente noutros sistemas baseados em UNIX.

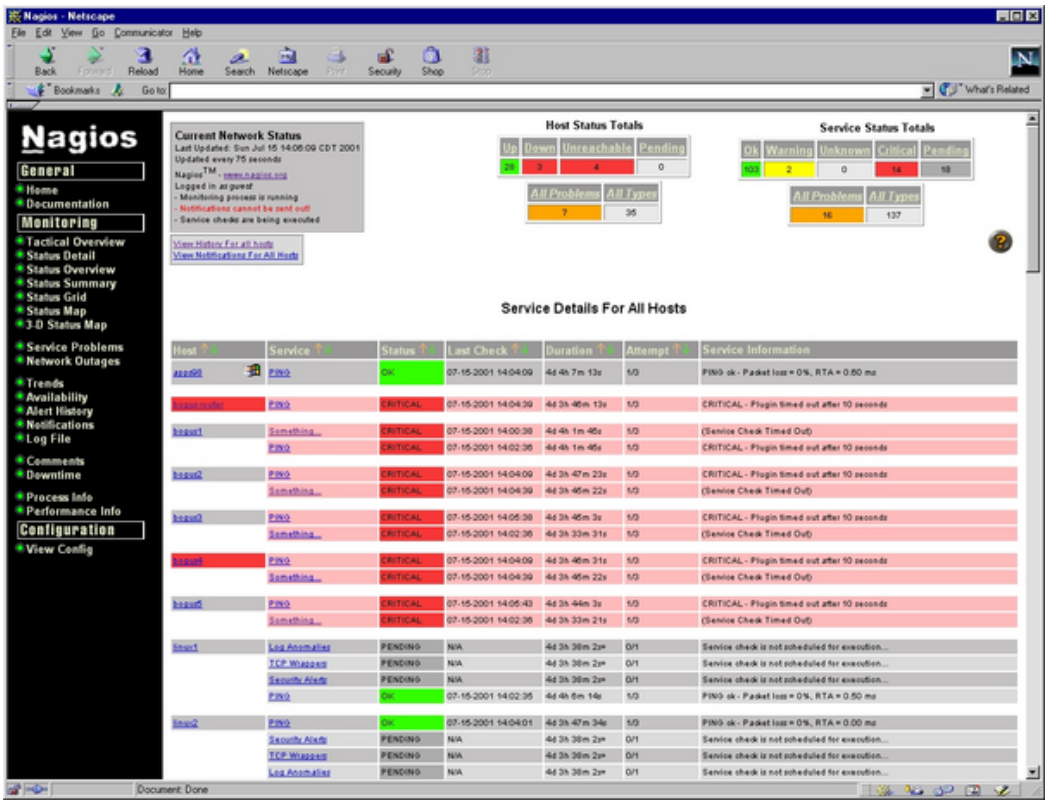


Figura 34 – Interface *Web* do Nagios

Principais características do sistema:

- Monitorização de serviços de rede (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);

- Monitorização de recursos de computadores ou equipamentos de rede (carga do processador, uso de disco, *logs* do sistema) na maioria dos sistemas operacionais com suporte a rede (mesmo o Microsoft Windows com o *plug-in* NRPE_NT);

- Monitorização remota suportada através de túneis encriptados SSH ou SSL;

-Desenvolvimento simples de *plug-ins* que permitem aos utilizadores criar facilmente os seus próprios modos de monitorização e em função das suas necessidades, usando qualquer ferramenta de desenvolvimento (Bash, C, Perl, Python, PHP, C#, *etc.*);

- Plano de atendimento a serviços;

- Capacidade de definir a rede hierarquicamente designando equipamentos "pai" e permitindo a distinção entre os equipamentos que estão indisponíveis daqueles que são inalcançáveis;

-Capacidade de notificar quando um serviço ou equipamento apresenta problemas e quando o problema é resolvido (via *email*, *pager*, SMS ou qualquer outro meio definido pelo utilizador por *plug-in*);

-Capacidade de definir processadores de eventos que executam tarefas em situações pré-determinadas ou realizam a resolução pró-activa de problemas;

- Recuperação automática de histórico;

-Suporte para a implementação de monitorização redundante;

-Excelente interface *Web* para visualização do actual estado da rede, notificações, histórico de problemas, arquivos de *log*, *etc*.;

As capacidades do Nagios podem ser aumentadas com a instalação de *addons* e ferramentas adicionais (ver tabela seguinte) [42].

Tabela 3 – Tabela de *addons* do Nagios

| Nome da Ferramenta ou *Addon* | Descrição |
|---|---|
| ***NagVis*** | *Addon* para a visualização de resultados de monitorização |
| ***NagCon*** | Consola de monitorização para UNIX |
| ***check_nagios_summary*** | Permite fazer a monitorização distribuída utilizando o Nagios |
| ***NagIRCBot*** | Alerta para a mudança de estado do Nagios no IRC |

| | |
|---|---|
| ***NagiosQL*** | Extensões de administração para Nagios 2.x |
| ***Monarch*** | Motor de *Web* para o controlo do Nagios 1.0 e 2.0 |
| ***Nag2web*** | Ferramenta de configuração para Nagios 2.0 |
| ***PerfParse*** | Base de dados para dados de desempenho |
| ***PNP*** | Ferramenta para mostrar graficamente dados de desempenho |
| ***Nagat*** | Ferramenta de administração para Nagios baseada em PHP |
| ***phpNagios*** | Ferramenta para configuração sem utilizar base de dados |
| ***NaWui*** | Ferramenta *Web* do utilizador para aceder ao Nagios |
| ***NagMin*** | Módulo instalado para a configuração do Nagios |
| ***mkncf*** | Ficheiro *Make* para ficheiros de configuração do Nagios |
| ***Speedview*** | Monitor do Nagios |
| ***N2RRD*** | Ferramenta para guardar e apresentar informação relativa ao desempenho do Nagios |
| ***NagiosGrapher*** | Ferramenta para integração de gráficos de desempenho |
| ***Fruity*** | Ferramenta de configuração baseada em PHP |
| ***Opsview*** | Ferramenta de configuração e monitorização com suporte para SNMP |
| ***NagiosChecker*** | Extensão do Firefox para monitorização de sistemas controlados pelo Nagios |
| ***Sentinet3*** | Aplicação IT baseada no Nagios |

Este gestor de rede só pode ser implementado em plataformas UNIX, tal como o Linux, precisando somente de um compilador de C (gcc). Para a utilização de CGI no navegador *Web* é necessário ainda instalar um *webserver* (o Apache preferencialmente) e a biblioteca gd de Thomas Boutell [43].

## 2.9 *Software* de Gestão de Rede na Indústria

No sentido de perceber que tipo de gestores de dispositivos de redes são utilizados por empresas concorrentes da EFACEC, foi elaborada uma pesquisa sobre este tipo de informação. Embora, na maioria das vezes, esta informação não seja disponibilizada, foram encontradas descrições de algumas das plataformas utilizadas.

**eWON**

A eWON utiliza para as suas famílias de *gateways* uma ligação a um servidor eSYNC.

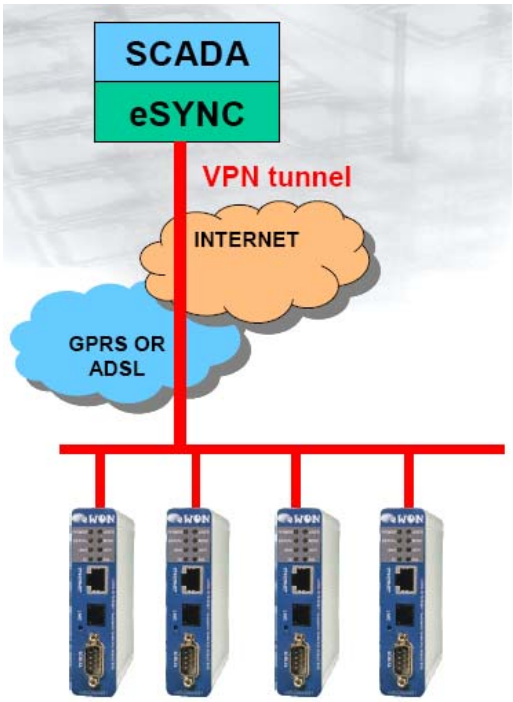


Figura 35 – Hierarquia dos produtos da eWON

Este servidor tem como características:

- Servidor de VPN;
- Gestão de endereços IP VPN, incluindo tabela de encaminhamento;
- Base de dados dos utilizadores e dos equipamentos eWON;
- Base de dados e gestão PKI;
- Apache, MySQL e OpenVPN integrados.


Figura 36 – Aspecto do serviço *Web* oferecido pelo eSYNC

## Tyco Electronics Energy

A *Galaxy Gateway* da Tyco Electronics Energy oferece suporte para sistemas operativos *standards* para gestão de múltiplos componentes, tais como o HP OpenView – Network Node Manager e Lucent One Vision.

A Tyco Electronics Energy desenvolveu uma aplicação para gestão dos seus produtos de potência. A aplicação chama-se Galaxy Manager e é uma aplicação desenvolvida em plataforma Windows.


Figura 37 – Página inicial do Galaxy Manager

Desenhado para ir de encontro às necessidades das operações de manutenção e controlo de arquitecturas de potência, o Galaxy Manager é um ponto central de recolha, monitorização, análise e controlo de informação. É uma solução com uma

arquitectura aberta baseada nos *standards* da Microsoft, que utiliza o protocolo de gestão de rede SNMP v2 para obter informação de alarmes para um servidor centralizado. Esta solução comunica com cada rede através de uma grande variedade de protocolos, incluindo TCP/IP, modem, Microsoft Visual Basic e Java, bases de dados ODBC e OLE para comunicações de controlo de processo (OPC) [45].

Apresenta uma janela de autenticação e a área de administrador que permite a gestão de utilizadores, *passwords*, níveis de acesso e configuração de endereço de *email* do servidor. Um mapa geográfico com representação da localização dos sistemas é apresentado, com informação geral sobre estado dos alarmes.


Figura 38 – Mapa do Galaxy Manager

Permite aceder à informação sobre os alarmes activados, ver o histórico de alarmes, ter acesso a ferramentas de engenharia (gráficos de tendência) e à configuração de cabos. Oferece ainda o acesso a informação detalhada sobre os sistemas que gere [46].

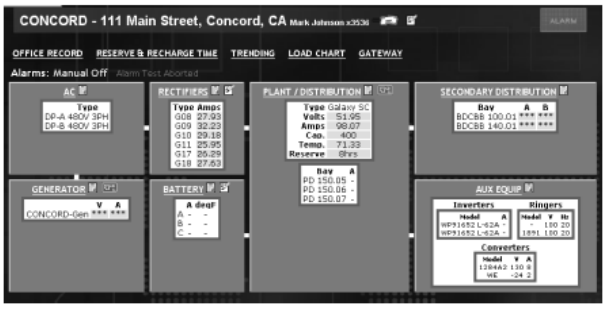


Figura 39 – Painel com informação de equipamentos


Figura 40 – Janela de alarmes activos

## SHAFT Power Systems

A SHAFT Power Systems disponibiliza, para a sua família de produtos de controlo de potência, o *WinSite*. O WinSite é um *software* baseado em Windows, desenvolvido para a monitorização e análise de uma forma simples e rápida do estado de equipamentos baseados nos módulos de supervisão da SHAFT Power Systems (ACM1D, CCU e NRC50). Fornece um modo de gerir eficientemente e hierarquicamente os dados provindos dos equipamentos.

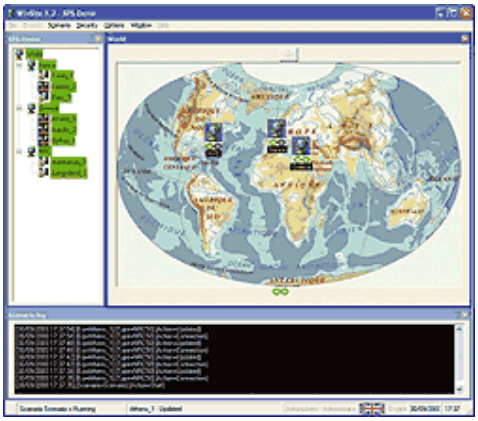

Figura 41 – SAFT WinSite

O WinSite pode:

- Automaticamente estabelecer conexões com equipamentos, de acordo com as definições do utilizador, e colectar informação principal de estado do dito equipamento;
- Aguardar por comunicações de outros equipamentos que podem enviar automaticamente as mudanças no seu estado;

Lidar com conexões do tipo:

- Local (RS-232/RS-485);
- Modem;
- TCP/IP (assumindo que o equipamento remoto está dotado de um sistema de comunicações.

Fornece um mapa com as localizações hierárquicas de cada equipamento (a que grupo pertencem, *etc.*) e permite a definição de tantos níveis de equipamentos quantos os necessários. Um gestor inteligente de comunicações é ainda capaz de se conectar aos equipamentos e interromper o *polling* efectuado ao conjunto de equipamentos presente na rede.

*Executar um cenário*

O MapView mostra uma imagem onde os ícones de equipamentos são colocados. Quando um cenário é executado, o WinSite estabelece a comunicação com o equipamento apropriado e retorna a informação do seu estado.

As visualizações são refrescadas de acordo com o estado do equipamento, utilizando-se uma codificação por cor simples que reporta:

- O estado da comunicação;
- O estado do equipamento em si.

Quando o equipamento se desactiva, é possível inspeccionar a lista de alarmes. Se for necessário um diagnóstico mais detalhado, o *software* de supervisão (tal como o WinSparc ou Win1d3) pode ser lançado directamente do WinSite para a se conectar ao equipamento.

*Requisitos Mínimos da Plataforma Windows*

Para que o *software* possa ser instalado, são necessários patamares mínimos em termos de suporte:

- Sistema Operativo: Microsoft Windows NT4, Windows 98, Windows 2000 ou XP;
- Memória RAM: 64 MB;
- Espaço em disco: 20 MB
- Monitor: SVGA com 256 cores;
- Uma porta série para comunicações de 19 200 baud (RS-232 ou RS-485);
- Um modem para comunicação remota com equipamento;
- Interface Ethernet para comunicação através de rede TCP/IP;

O *software* suporta ainda três línguas: Inglês, Espanhol e Francês. Tem três níveis de acesso implementados:

- Utilizador: Para operações de leitura;
- Super Utilizador: Para iniciar um cenário;
- Administrador: Acesso completo para efectuar todo o tipo de operações [47];

**EMERSON**

A EMERSON disponibiliza, no seu ramo de gestão de redes de energia, três tipos de *software*. O primeiro é o Emerson Network Energy Network (ENEC) que foi desenvolvido para o mercado sul-americano. Trata-se de um produto para monitorização remota de sistemas de energia, sistemas de climatização, *etc.*

O ENEC fornece funções de supervisão de uma rede de gestão, utilizando a *Web*. O ENEC é distribuído, escalar, fácil de utilizar e oferece aos seus utilizadores o total controlo sobre dezenas de equipamentos e sobre o seu sistema de alarmes. É baseado em *standards* da indústria tais como o Oracle, Java, HTML, SSL e Windows. Suporta protocolos de comunicação tais como o TCP/IP.

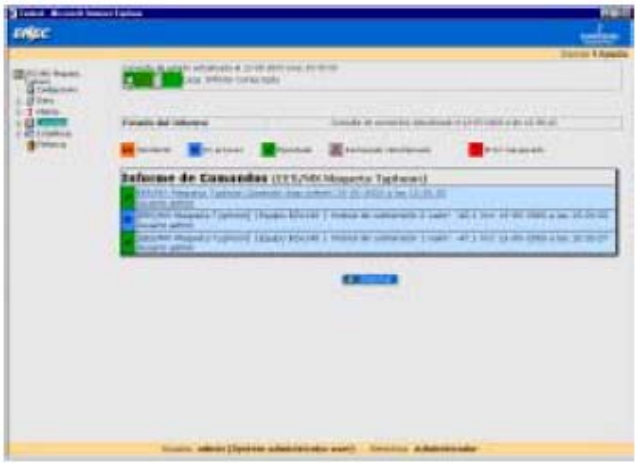

Figura 42 – Envio de comandos

O ENEC pode satisfazer tanto um cliente que controle apenas cinco equipamentos ou locais diferentes como clientes que controlem várias dezenas de equipamentos. Permite a gestão de:

- Rectificadores e distribuidores de tensão DC;
- Fornecedores de tensão AC;
- Fornecedores de tensão DC;
- Geradores;

- Refrigeradores.

*Características:*

Pode ser executado em qualquer plataforma e com qualquer interface *Web*. O cliente não necessita de instalar qualquer tipo de *software* adicional além de um navegador *Web* tal como o Internet Explorer ou o Mozilla para aceder a todos os serviços do sistema.


Figura 43 – Navegação por mapas

Permite ser acedido a partir de qualquer parte do mundo através do seu servidor WEB. Permite ser acedido ao mesmo tempo por vários utilizadores sem criar conflito de gestão ou no acesso à informação ou equipamentos. O sistema pode ser instalado em várias máquinas, permitindo a redundância em caso de falha de uma das máquinas. Neste caso, a máquina de reserva toma controlo sobre o sistema, substituindo a máquina que falhou. Permite a comunicação com equipamentos de outros fabricantes através de XML e TCP/IP para partilha de informação.

Em termos de segurança o ENEC utiliza o protocolo SSL para garantir uma ligação segura entre o equipamento e o servidor. A base de dados do sistema é desenvolvida em Oracle DB. Esta base de dados permite a gestão de um número ilimitado de lugares e equipamentos. Os protocolos de comunicação são tão variados como o IP, V24, Modem PSTN e GSM.

A gestão do estado dos equipamentos é suportada por um processo de *polling* aos objectos/equipamentos definidos na mesma. Os alarmes ou mudança de estado

dos vários equipamentos é automaticamente enviado para o ENEC. Com estas informações o ENEC activa uma série de processos pré-definidos pelo administrador do sistema, que podem englobar o envio de *emails* e SMS para o operador mais próximo na árvore hierárquica. O objectivo principal é garantir que o alarme seja tratado correctamente.

O ENEC apresenta a informação ao operador de forma instantânea e fácil de interpretar para que este possa actuar de forma rápida e eficiente, evitando o acesso a informação secundária desnecessária. A página *Web* apresenta a informação de estado e alarmes de uma forma simples e colorida para percepção imediata da mudança de estado dos equipamentos.

Figura 44 – Navegação por árvore

É possível ainda ver informação relativa a evolução de certos aspectos do equipamento, tal como a tensão ou a temperatura durante testes ou períodos de tempo pré-definidos [48].

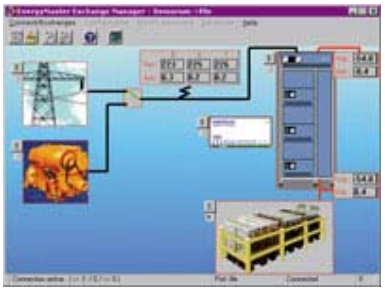

Figura 45 – EXMG

Outro produto da família de produtos da EMERSON é o EXMG que foi desenvolvido para gerir o equipamento da EMERSON Energy e Energy Site Management (ESM). O sistema permite operações tanto a nível local como a nível

remoto, permitindo a realização de quase todo o tipo de operações directamente sobre o equipamento, sem a necessidade de efectuar uma deslocação ao local.

*Aplicações*

- Gestor Base: Este gestor cobre a gestão de alarmes, incluindo o atendimento de alarmes e o envio de avisos ao utilizador/operador.

- Gestão de Desempenho: Esta aplicação fornece ao utilizador funções de analise do estado dos equipamentos controlados.

- Gestão de Elementos: Esta aplicação permite configurar e controlar os equipamentos através de operações tais como modificar valores, alarmes, *etc.*

- Gestão de Configuração: Esta aplicação gere as configurações do próprio EXMG, permitindo a gestão de locais, equipamentos, *etc.*

- Gestão de Apresentação: Esta aplicação permite gerir a apresentação gráfica e a interface do utilizador.

Características fundamentais:

- Aplicação Windows: A aplicação foi desenvolvida para ser executada numa plataforma Windows;

- Solução Cliente/Servidor: A aplicação EXMG permite vários utilizadores distintos ligarem-se à máquina em simultâneo, acedendo à mesma informação gerida por um servidor de dados comum;

- *Polling* – EXMG suporta tanto operações de *polling* agendadas automaticamente como manuais. Para o *polling* automático há servidores de comunicação separados que fazem o *poll* simultâneo e contínuo de múltiplos equipamentos, de forma a manter a informação na base de dados sempre actualizada;

- Informação Centralizada – A EXMG oferece ao utilizador informação instantânea sobre o estado e informação de alarme dos diferentes equipamentos.

- Testes Remotos e Análise – Ao accionar um teste ou análise de resultados num equipamento, pode-se analisar a tendência e evolução de um determinado parâmetro numa máquina, possibilitando ao operador inteirar-se da sua operacionalidade [49].

O terceiro produto da EMERSON para gestão da sua rede é o Energy Management Application (EMAS). Este *software* é um produto desenvolvido para controlo e gestão de sistemas de potência, sistemas de climatização e produtos relativos a soluções no campo da energia. O EMAS providencia funções de supervisão ao nível da gestão de rede e introduz grandes melhoramentos nas actividades de manutenção e disponibilidade da rede. O EMAS é um produto baseado nos *standards* da indústria (*e.g.,* o HP OpenView e o HP-UNIX) para assegurar um bom desempenho. Suporta protocolos de comunicação tais como o SNMP, TCP/IP e X.25.

Figura 46 - EMAS

Baseado em HP-OpenView – O EMAS é baseado num *standard* popular na indústria de controlo, o HP Openview Network Node Manager, que apresenta uma interface amigável e conhecido. Utiliza uma aplicação para visualização de informação denominada de Wingz, muito conhecida no mundo Unix, para fazer a

apresentação de informação relativa aos equipamentos. Utiliza um conjunto de métodos de comunicação amplamente conhecidos, tais como o IP, v.24 e Modem, *etc.*, e, através de *polling*, faz a actualização de todos os equipamentos.

Os Alarmes e/ou mudanças de estado são automaticamente enviadas para o EMAS. A informação sobre alarmes é automaticamente apresentada ao utilizador, sob uma forma muito simples e eficaz, para que este possa filtrar rapidamente o que necessita e actuar em conformidade [50];

**Gamatronic**

Outra companhia, a Gamatronic disponibiliza o *Element Management System* (GeMSi). Este *software* providência a monitorização em tempo real de alterações de estado de até 400 unidades de controlo em diferentes localizações recebendo avisos de notificações (*e.g.* alertas e alarmes) e enviando notificações via *email*, telemóvel ou para o centro de controlo.

O GeMSi pode também ser utilizado para enviar comandos para várias unidades. Mantém uma comunicação bidireccional com unidades, cartas de interface e alimentadores (através de *software* de PSM).

O GeMSi permite a recepção de actualizações de dados em tempo real de sistemas de potência e controla-os de acordo com o estipulado nas configurações. O GeMSi usa uma estrutura hierárquica que providencia uma visão global sobre todos os equipamentos num mapa geral em que estão representados os grupos de equipamentos e alarmes activos (se for o caso). Neste mapa geral é possível manter as resoluções e ver de uma forma mais próxima os equipamentos ou grupos de equipamentos, de forma a poder monitorizá-los individualmente. Esta arquitectura permite a observação de todos os sistemas de potência de um determinado grupo.

Qualquer entrada detectada por controlador de UPS activa automaticamente uma luz de alarme indicativa da gravidade e estado, além de uma mensagem de alarme a especificar o problema. A luz de alarme aparece na caixa relativa a alarmes

e no mapa, sob o equipamento com falha. É adicionada ao histórico de alarmes para posterior análise.

*Espião de Parâmetros*

O *software* GeMSi pode ser configurado para servir como um espião de parâmetros e levar a cabo uma extensa depuração de erros e investigar as condições específicas que os provocam. Por exemplo, o GeMSi pode instruir uma das unidades de controlo sob sua gestão para amostrar num intervalo de tempo específico um determinado parâmetro e guardá-lo na sua base de dados. A informação pode então ser analisada *off-line* e comparada com outros parâmetros obtidos.

*Notificação de Pré-alarme*

Em adição ao envio de alarmes quando os valores excedem os valores recomendados, o GeMSi envia notificações de valores anormais, mesmo que estes não ultrapassem os valores especificados para os alarmes. O GeMSi permite fazer a amostragem de determinados valores ao longo do tempo para "aprender" qual a gama de valores normais, estando alerta para flutuações fora dessa gama de valores.

Características:

- Unidades AC, unidades DC e gestores de energia;
- Múltiplos sistemas de gestão debaixo da mesma plataforma;
- Indicadores em tempo real;
- Arquitectura para multiutilizador, com um esquema de segurança;
- Histórico de utilizadores e sistemas;
- Parâmetros e definições de página alteráveis para cada tipo de utilizador;
- Plataforma NMS;

- Notificações por SMS, *email*, *pop-up*, *net message* e mensagem áudio;
- Notificação de alteração de estado;
- Lembrete automático de manutenção;
- Navegador *Web* interno;
- Comunicações por Modem, SNMP, PPP, SMS e HTTP.

**MGE**

A MGE apresenta o Enterprise Power Manager como ferramenta de controlo e monitorização de redes de UPS. Esta ferramenta utiliza a representação gráfica através de um navegador de *Web* para facilitar a supervisão eléctrica do sistema. As definições de visualização das UPS podem ser alteradas a partir das definições mais críticas do sistema. Os alarmes podem ser centralizados e transmitidos, se necessário, através de *email* ou SMS. O histórico de funcionamento das redes de UPS permite fazer uma gestão preventiva da rede. As manutenções podem ser marcadas e automatizadas.

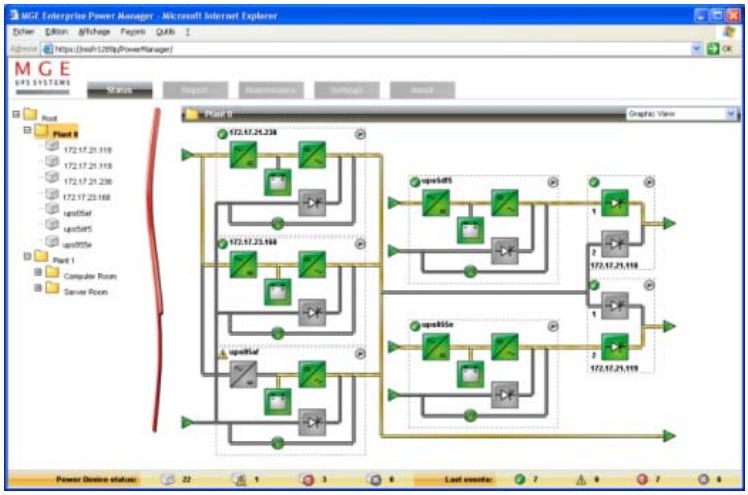


Figura 47 – Aspecto do Enterprise Power Manager

Após a sua instalação no sistema, o Enterprise Power Manager leva a cabo uma inspecção da rede para descobrir todos os sistemas de UPS ligados, todos os servidores a utilizar o Network Shutdown Module e outras unidades de gestão de

potência. O resultado é apresentado num *layout* configurável, de acordo com o tipo de UPS, localização, estado, *etc*.

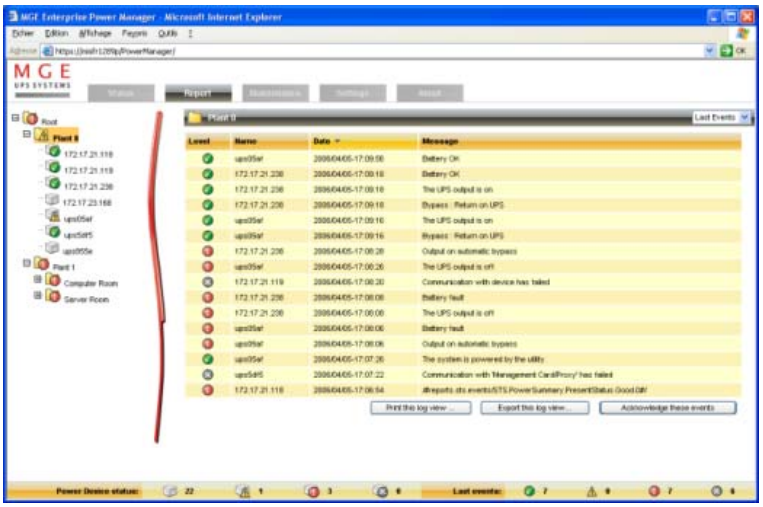

Figura 48 – Aspecto do *layout*

Clicando no *layout* de uma UPS tem-se acesso a informação detalhada acerca dos parâmetros de operação e configuração numa janela dedicada. As arquitecturas complexas constituídas por múltiplas UPS podem também ser facilmente geridas e controladas. Pode-se ter acesso a detalhes de relatórios estatísticos, protocolos de segurança adoptados (SSL) e gestão de vários níveis de *password* (administrador, utilizador, *etc.*).

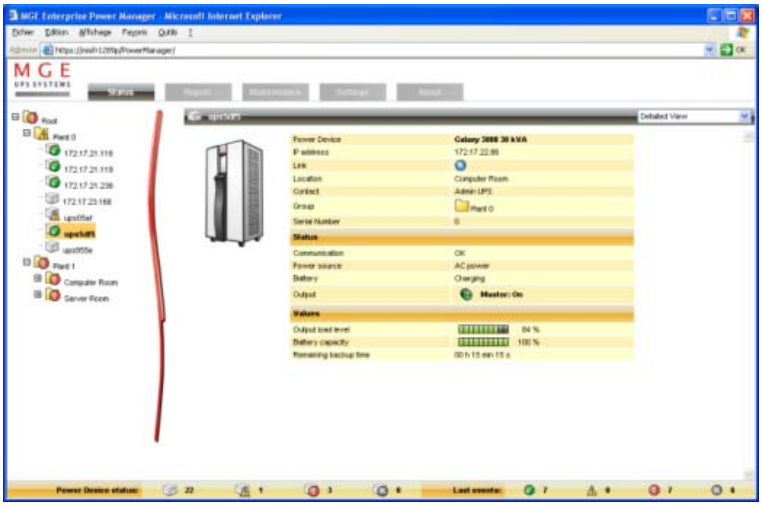

Figura 49 – Apresentação gráfica de uma UPS

# 3 Análise de Requisitos

Este projecto insere-se numa encomenda específica de um cliente da EFACEC Sistemas de Electrónica, S.A. para um produto ou família de produtos da linha Efapower.

O cliente deseja adquirir um serviço que permita a monitorização e controlo remoto de um ou mais CIB da EFACEC. A EFACEC Sistemas de Electrónica possui já um servidor que disponibiliza estas funcionalidades, que foi construído sobre o sistema operativo Linux.

Algumas das características deste servidor existente vão de encontro às necessidades do cliente, mas há, contudo características adicionais que não estão disponíveis. Neste capítulo será explicitado o conjunto e características que este produto tem e quais as novas funcionalidades que se pretendem implementar. Será apresentado o conjunto de requisitos/funcionalidades que o novo produto deverá apresentar. A informação detalhada relativa aos componentes físicos do sistema tais como os bastidores CIB, PSM e SNMP é apresentada num capítulo posterior denominado de Descrição do Suporte Físico.

## 3.1 Plataforma Existente

A EFACEC - Sistemas de Electrónica, ramo de Sistemas de Alimentação, desenvolveu um conjunto de produtos na gama de fornecimento de energia ininterrupta, entre os quais se destacam os Carregadores Industriais de Baterias (CIB), com capacidade para fornecer grandes quantidades de energia, e as Unidades de Alimentação Ininterrupta (UPS) para fornecer menor quantidade de energia durante períodos de tempo mais curtos.

O controlo de um CIB é efectuado através de um controlador embutido no bastidor denominado PSM que monitoriza e faz o controlo directo sobre o disparo dos tirístores, tensões máximas e mínimas admissíveis, *etc.* Este dispositivo tem uma interface com o exterior através de um LCD e respectivos botões de comando para

gestão local e de ligações via RS-232 e via linha telefónica (PSTN ou GSM) para controlo remoto. Este PSM pode ser acedido através de Telnet, SNMP e inclui um *webserver* embutido.

A EFACEC – Sistemas de Electrónica, S.A. desenvolveu, em conjunto com esta linha de produtos, um servidor de páginas *Web* externo denominado **Efapower WebServer**. Trata-se de um PC com o sistema operativo Linux onde foi instalado e desenvolvido um *webserver* especializado. Este *webserver* está concebido para se ligar a vários CIB e permitir o seu controlo e monitorização. É ainda possível guardar os dados destes dispositivos numa base de dados.

Especificando as funções deste *webserver* temos:

- Ligação através de Ethernet 10/100 Mb/s;
- Ligação por Telnet;
- Ligação por SNMP;
- Envio de notificações de alarmes por correio electrónico;
- Sistema de validação de utilização com vários níveis de acesso;
- Gestão de utilizadores;
- Gestão de grupos de utilizadores;
- Registo de acessos ao servidor;
- Gestão de grupos de equipamentos (adição/remoção);
- Acesso a valores de medidas por componente;
- Histórico de medidas e alarmes dos vários componentes;
- Sinóptico configurável;
- Sinóptico por CIB;

- Actualizações de valores em tempo real;
- Monitorização e controlo de rectificadores, baterias e entradas/saídas auxiliares;
- Definição de parâmetros de funcionamento para cada componente.

## 3.2 Requisitos/Funcionalidades

O Efapower WebServer apresenta muitas características operacionais válidas para a maioria dos clientes, mas não está preparado para redes que não possuam ligações de 10/100 Mb/s. Alguns clientes possuem redes de telecomunicações mais antigas e ainda utilizam modems analógicos. De forma a adaptar o produto às limitações destes clientes, a conexão através de modem analógico deverá passar a ser suportada.

Outro requisito é o sistema operativo onde o servidor é disponibilizado. O cliente deseja que o *webserver* seja executado em sistemas operativos Microsoft Windows. Esta questão obriga a desenvolver uma aplicação para plataformas Windows.

Neste capítulo descreve-se a melhor solução técnica possível para um servidor deste tipo para os CIB da EFACEC – Sistemas de Electrónica, S.A. A solução será especificada sobre o ponto de vista dos tipos de ligações que deverá possuir, protocolos suportados, segurança, funcionalidades, soluções de engenharia e expansões possíveis.

A solução será dividida por tipo de equipamento a suportar, e tendo em conta a arquitectura de rede em que estará instalada.

Tabela 4 – Requisitos gerais do *webserver*

| *Característica* | *Função* | *Descrição* |
|---|---|---|
| *Ligações* | RJ45 (10/100 Base-T)<br>RS-232/422/485<br>Wi-Fi<br>GSM | Interface Ethernet<br>Interface Série<br>Interface *Wireless*<br>Interface GPRS |

| | | |
|---|---|---|
| *Protocolos* | ARP | |
| | FTP | |
| | IP/ICMP | |
| | DNS | |
| | SMTP | Com e sem autenticação |
| | DHCP | Cliente e servidor |
| | NTP | Cliente |
| | PPP | Cliente e servidor |
| | PPPoE | Cliente e servidor |
| | TCP | |
| | UDP | |
| | SSL | Versão 2 e 3 |
| | TLS | Versão 1 |
| | RFC-2217 | Suporte Telnet |
| | SSH | Versão 1 e 2 |
| | Telnet | |
| | HTTP | |
| | HTTPS | |
| | SNMP | Versão 1 e 2 |
| *Segurança* | *Username* e *Password* | Autenticação |
| | HTTPS | Ligação segura |
| | SSL v2 e v3 | |
| | TLS v1 | |
| | 3DES | |
| | RC4 | |
| | Filtragem de IP | *Firewall* |
| | SCP | |
| *Funcionalidades* | Alertas | *Email*/SMS/*Pager*/ *Trap* SNMP |
| | Níveis de acesso | 3 Níveis |
| | Gestão de Utilizadores | |
| | Gestão de Grupos | Cada grupo refere-se a um nível de acesso |
| | Gestão de Equipamentos | Adição/remoção de equipamentos |
| | Histórico | Medidas/Acessos/Alarmes |
| | *Webserver* | |
| *Gráficos* | Sinóptico | Configurável |
| | Actualização de valores | Em tempo real |
| | Configuração de *Webserver* | Alteração do aspecto pelo administrador |
| *Monitorização* | Baterias | Tensão |
| | | Corrente |
| | | Temperatura |
| | Rectificadores | Tensão |
| | | Corrente |
| | Alarmes | Por prioridade |
| | Histórico | Base de dados SQL |

| | | |
|---|---|---|
| *Memória* | Ficheiros de Configuração | *Webserver*<br>CIB<br>UPS |
| *Expansão* | Expansão Horizontal<br>Expansão Vertical<br>Integração com SCADA | Inserir tipos de componentes<br>Inserir componentes do mesmo tipo<br>Sistema de controlo e monitorização |
| *Engenharia* | Gráficos de desempenho | Corrente/tempo<br>Tensão/tempo<br>Temperatura/tempo<br>Descarga/tempo<br>Recarga/tempo |
| | Gráfico de previsibilidade | Descarga/tempo<br>Recarga/tempo |
| | Guia de procedimentos | Alertas de possíveis resoluções para problemas que surjam |

Esta tabela engloba, de uma forma geral, todas as funcionalidades que o *webserver* genérico deveria ter. Contudo, será necessário particularizar para cada tipo de ligação específico e para cada tipo de equipamento, pois, desde logo, há diferentes requisitos em jogo.

Por exemplo, faz sentido implementar um módulo de expansão do servidor para que se possa ligar a uma rede Wi-Fi (*wireless*) para controlo e monitorização de uma UPS. Este tipo de equipamento não costuma ser vital e as questões de segurança habitualmente colocadas pelas redes Wi-Fi não são problemáticas. Além disso, e porque as UPS se encontram muitas vezes em escritórios e outros lugares confinados, a questão da utilização de tecnologia *wireless* faz todo o sentido. Com a expansão deste tipo de redes, é natural que venhamos a verificar um aumento do número de produtos que disponibilizem este meio de conexão.

Contudo o Wi-Fi não faz sentido quando se fala de monitorização e controlo de CIB. Este tipo de dispositivo encontra-se em locais remotos e no exterior onde apenas uma rede por cabo pode chegar. As ligações de GSM permitem ligações sem fios mas ainda não estão disponibilizadas neste tipo de equipamentos da EFACEC. Além disso a questão da segurança é vital. Estes são equipamentos são críticos para os sistemas que alimentam, não se podendo correr riscos de quebra de segurança.

Assim, é natural que nem os fabricantes, nem os clientes optem pela utilização, de Wi-Fi neste caso mesmo quando esta está disponível.

### 3.2.1 Protocolos Utilizados pelo CIB da Efapower

Um CIB engloba, normalmente, dois módulos: o PSM e o SNMP. O módulo PSM, enquanto controlador, tem uma saída de dados RS-232 (interface série) e o módulo SNMP tem uma interface Ethernet e disponibiliza os dados via SNMP. A estrutura em que estes dados são disponibilizados é descrita de seguida.

#### 3.2.1.1 Interface Série

A comunicação série PC-PSM é realizada sobre um protocolo que define um conjunto de mensagens passíveis de serem trocadas.

Todas as mensagem são compostas por:

- Um byte que identifica o tipo de mensagem;
- Dois bytes que indicam o comprimento da zona de dados da mensagem;
- Opcionalmente, *n* bytes de dados que formam a zona de dados da mensagem;
- Dois bytes de CRC – *Cycle Redundancy Check* -(byte menos significativo primeiro).

Segue-se o esquema da sintaxe referida:


Figura 50 – Trama geral do protocolo EFACEC

A única excepção a este formato é a mensagem NACK (*Not Acknowledge*), em que a zona de dados da mensagem tem comprimento fixo (1 B) e, portanto, os dois bytes (2 B) que indicam o comprimento da zona de dados não existem.

#### 3.2.1.2 Interface Ethernet

A comunicação via interface Ethernet é efectuada sobre SNMP (*Simple Network Management Protocol).* O SNMP é um *standard* largamente utilizado para gestão remota de dispositivos de rede (*routers, bridges, etc.*), que é baseado num modelo gestor/agente simples (*simple*), uma vez que o agente requer pouca complexidade de *software.* Por esta razão, este protocolo é utilizado para comunicar com vários dispositivos de *hardware* desenvolvidos pela EFACEC S.E., neste caso o módulo SNMP ligado ao PSM.

O módulo *SNMP* existente no CIB implementa o protocolo SNMPv1, cujas características são agora explicitadas.

O Protocolo SNMP utiliza cinco tipos básicos de mensagens:

- *Get* (operação de leitura);
- *Get next* (operação de requisição do valor seguinte);
- *Set* (operação de escrita);
- *Trap* (operação assíncrona de envio de notificações/alarmes por parte do dispositivo);
- *Get-Response* (mensagem enviada ao gestor com a informação requerida ou, em caso de falha, o código de erro associado).

Todas estas mensagens partilham a seguinte estrutura de mensagem:


Figura 51 – Cabeçalho da mensagem SNMPv1

Elementos constituintes do cabeçalho:

**Versão** – Versão do SNMP utilizado, no caso deste projecto Versão 1;

**Comunidade** – Define o acesso para um grupo/comunidade de NMS. Este campo é utilizado como uma forma básica de autenticação

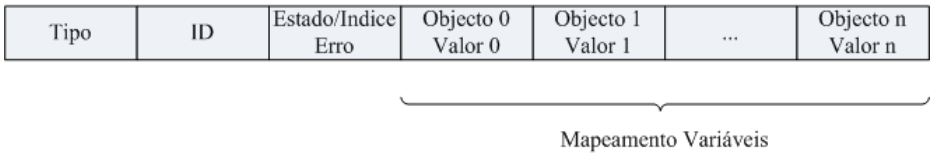


Figura 52 – Elementos constituintes PDU SNMPv1

Elementos constituintes da *Protocol Data Unit* (PDU):

- **Tipo PDU** – Identifica o tipo de unidade de protocolo;
- **Request ID** – Associa os pedidos SNMP com respostas;
- **Error status/index** - Somente a operação *response* define este campo, indicando o número de erros e o objecto que os causou. Nos outros tipos de mensagens este campo é nulo;
- **Mapeamento Variáveis** – No campo de dados da PDU os objectos são associados aos seus valores correntes. Associa um dado objecto com o seu valor actual. Nos tipos de mensagem Get/GetNext o valor é ignorado;

Todas as mensagens contêm o mesmo formato de PDU, com a excepção da mensagem *trap*.


Figura 53 – Trama *Trap* SNMP v1

Elementos constituintes da PDU:

- **Empresa** - Identifica o tipo de objecto gerido responsável pela criação da *trap*;

- **Endereço do agente -** Indica o endereço do objecto gerido responsável pela criação da *trap*;

- **Código *trap* genérico -** Indica um ou mais tipos de *trap* genéricos;

- **Relógio -** Indica o tempo que decorreu entre a última reiniciação da rede e a criação da *trap*;

- **Mapeamento Variáveis -** Campo de dados da PDU onde os objectivos são associados aos seus valores actuais. A implementação do protocolo SNMP foi realizada com o apoio da biblioteca *synapse* que fornece as funções e mecanismos necessários ao funcionamento deste protocolo.

**MIB**

Uma MIB é uma base de dados organizada de forma hierárquica que contém, um conjunto de informações de gestor de um conjunto de recursos, assemelhando-se a uma estrutura de dados encapsulada.

Esta estrutura de dados representa todos os valores que poderão ser acedidos através do protocolo SNMP, sendo constituída por objectos de gestão (objectos MIB) que comportam uma ou mais instâncias de objectos, que representam variáveis.

Existem dois tipos de objectos MIB, escalares e tabulares. O primeiro tipo refere-se a uma única instância, enquanto que o último representa uma tabela de múltiplas instâncias.

Um identificador de objecto identifica somente um objecto MIB na hierarquia MIB. A hierarquia MIB pode ser descrita como sendo uma árvore com uma raiz sem nome definido, cujos níveis são definidos por diversas organizações. Os níveis de topo pertencem a organizações que definem *standards,* enquanto que as de mais baixo nível podem derivar destas e implementar as variáveis necessárias ao seu funcionamento, ou então, derivar de um nó experimental se não obedecerem a qualquer *standard*.

### 3.2.2 Monitorização e Controlo por SNMP

Será adoptado um gestor de agentes de SNMP, seguindo a filosofia de gestão de redes de pacotes implementada OpenView NNM da HP e aproveitando os agentes de SNMP já instalados em cada PSM e SNMP. Este gestor de agentes de SNMP será responsável por manter um registo actualizado do número de componentes ligados em rede e por monitorizar o seu correcto funcionamento.

A solução a adoptar deverá ainda integrar informações úteis das MIB de SNMP (tais como identificação da máquina, medidas e estados) na base de dados da aplicação. Estes dados estarão disponíveis para o utilizador através da execução de pedidos específicos de valores da base de dados ou de actualizações automáticas, sendo os valores resultantes mostrados nas páginas disponibilizadas pelo *webserver* integrado na aplicação.

Deverá ser possível, através do servidor *Web* embutido, ter acesso ao estado de cada máquina na rede e ao registo de alarmes. Cada alerta de alarme ou falha na detecção de um componente da rede deverá desencadear um o conjunto de procedimentos configurados pelo utilizador/administrador do sistema. Neste grupo de procedimentos podem figurar alertas para um determinado endereço de correio electrónico, *traps* de SNMP, alertas por SMS, alertas sonoros, gráficos para o operador local da máquina de gestão, *etc.*

A própria aplicação desenvolvida deverá ter um agente de SNMP incorporado para poder ser integrada num sistema mais vasto de rede, com um gestor de rede de hierarquia superior ou para um acesso simples à sua identificação e dados.

### 3.2.3 Hierarquia do Sistema

Neste ponto será apresentada, de forma esquemática, a hierarquia do sistema a implementar, nomeadamente quais os dispositivos que se interligam e quais os níveis a que pertencem.

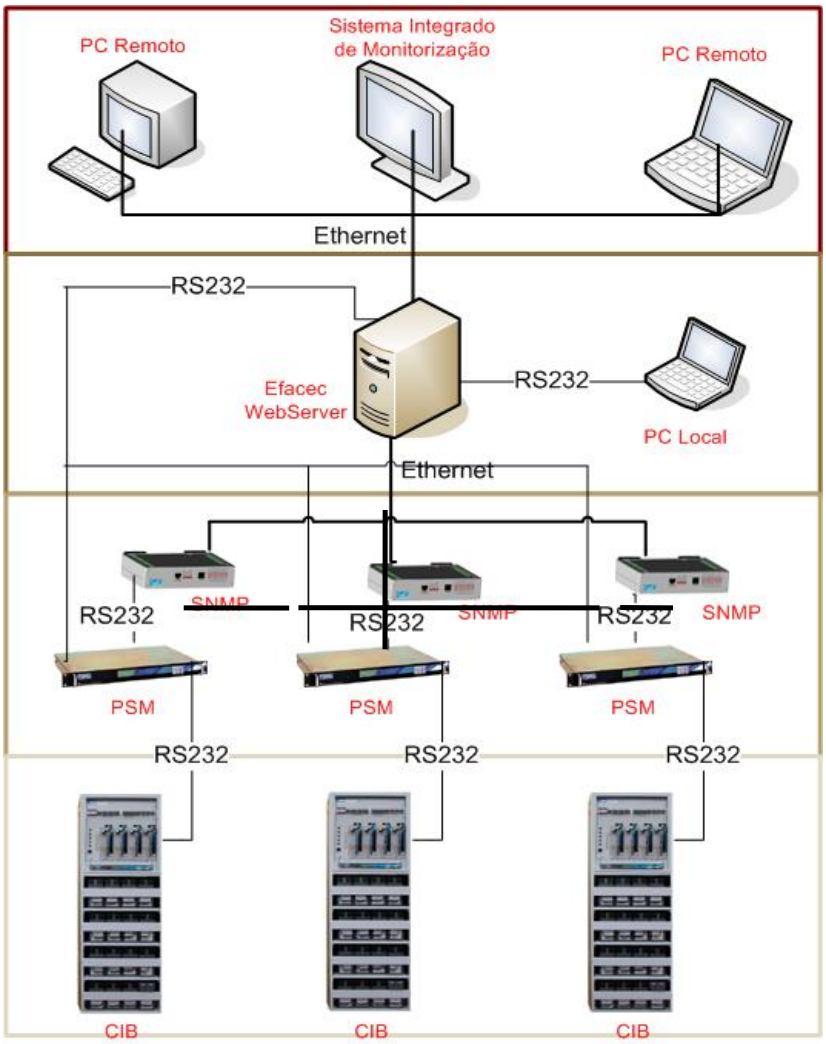


Figura 54 – Hierarquia de ligações

### 3.2.4 Tipos de Ligações Possíveis no Servidor

Para se definir a arquitectura a adoptar para o servidor é necessário estipular os tipos de ligações previstas. O servidor pode receber dados dos CIB, através das seguintes interfaces:

- Interface de Ethernet proveniente do módulo SNMP (RJ45);
- Interface *Dial-Up* proveniente de modem analógico externo (RJ11);
- Interface série RS-232 proveniente directamente do módulo PSM (Porta COM);

Assim, em termos esquemáticos, teremos:

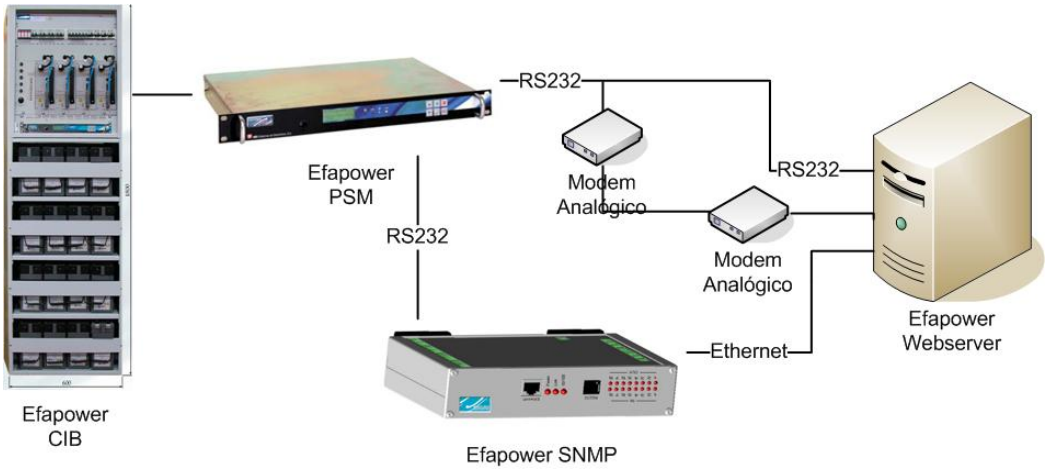


Figura 55 - Ligações de entrada possíveis para o servidor

Em termos de saída de dados teremos o mesmo tipo de ligações que para as entradas. Como iremos ver mais à frente nesta tese, a opção da ligação Wi-Fi (*wireless*) foi deixada propositadamente de fora no caso do servidor de CIB. Essa opção apenas seria considerada em servidores dedicados a UPS.

### 3.2.5 Suporte para Ligação Série

As características que o servidor deverá suportar dependerão do tipo de ligação que se efectue ao dispositivo, uma vez que esta definirá quais os protocolos suportados. A ligação série (ou porta COM) através de um conector RS-232, permitirá ligar localmente ao servidor e servirá para efectuar configurações do próprio servidor. Esta ligação é limitada em termos de protocolos suportados, aplicações e segurança. A opção de *webserver* não estará disponível, uma vez que esta utiliza o protocolo HTTP, apenas disponível para a interface Ethernet.

Figura 56 – Conector RS-232

Ligação Série:

*Protocolo de Rede:*

- TCP;

- UDP;

*Protocolos de segurança:*

- SSL versão 2 e 3;

- TLS versão 1;

*Configuração:*

- Telnet

Esta ligação apenas permite aceder à ferramenta de configuração Telnet do servidor para configuração ao nível do IP, máscara e *gateway*, definição de servidor de *emails*, correio electrónico de clientes, *etc.*

### 3.2.6 Suporte para Conexão de *Dial-up*

Para iniciar uma conexão de *dial-up* através de um modem analógico será necessário implementar um protocolo PPP para ligar a aplicação a um servidor de PPP. Esta conexão dotará a aplicação de uma conexão com suporte TCP, necessário para a implementação do protocolo de gestão SNMP.

A mesma lógica de ligação é necessária para os equipamentos a ser monitorizados, caso estes não estejam dotados de uma interface Ethernet. A ligação através de um modem torna-se, assim, fundamental para assegurar a conectividade deste tipo de equipamentos ao sistema de gestão e controlo remoto.

### 3.2.7 Suporte para Ethernet

O típico esquema de ligação deste servidor será feito através de interface Ethernet, pelos terminais RJ45 (ligação 10/100 Base-T).


Figura 57 – Conector RJ45

Nos esquemas seguintes apresentam-se exemplos dos tipos de ligações que a aplicação *Web* (Efapower WebServer) terá de suportar.

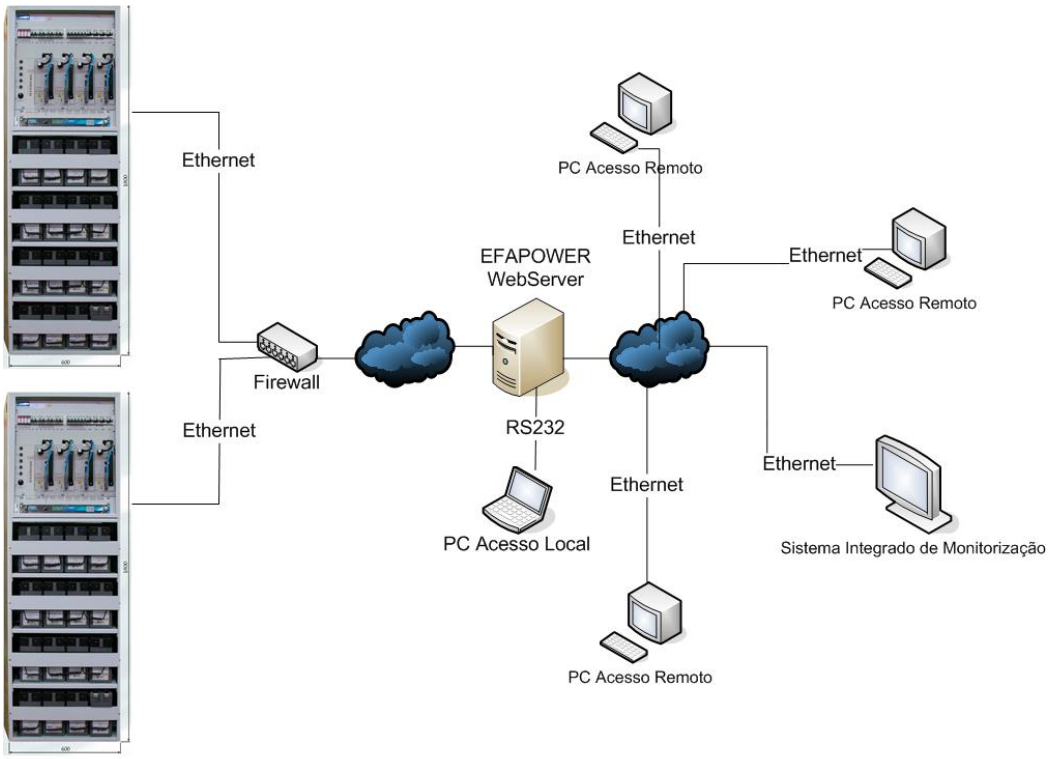


Figura 58 - Ligação por Ethernet

No primeiro caso, dois CIB ligam-se à Internet por intermédio de um *hub*. A aplicação *Web* disponibiliza ligação local (Porta COM) para operações de configuração e manutenção (através de Telnet) e disponibiliza os serviços de SNMP, servidor de HTTP, envio de *Emails*, *etc.* através da interface Ethernet.

No segundo caso, parte-se do princípio que a infra-estrutura do cliente apenas suporta a linha telefónica comum, com conectores RJ11, e que a conexão à Internet se deverá efectuar via modem. O servidor deverá suportar não só modem *Dial-Up*

(faixa estreita com acesso através de PPP, recorrendo a TCP/IP), mas também modem *Digital Subscriber Line* (DSL) (faixa larga com acesso por PPPoE).

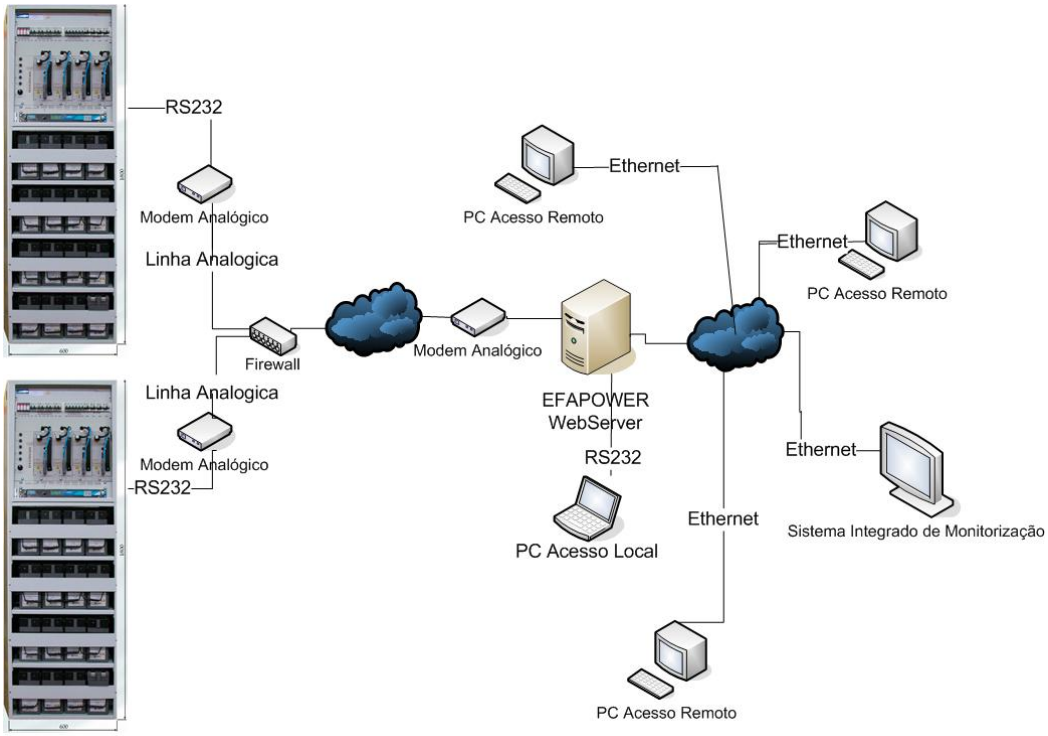


Figura 59 - Ligação por linha telefónica comum.

Assim, é possível definir as características e encadeamento das várias camadas de protocolos que este servidor deverá suportar através da interface Ethernet.

**<u>Ligação Ethernet:</u>**

*Protocolo de Rede:*

- IP/ICMP;
- DHCP;
- PPPoE;
- PPP;
- TCP;
- UDP.

*Protocolos de Segurança:*

- SSL versão 2 e 3;

- TLS versão 1.

*Configuração:*

- Telnet;

- SSH.

*Protocolos de Aplicações:*

- SMTP;

- NTP;

- HTTP;

- HTTPS;

- FTP;

- ARP;

- SNMP;

- DNS.

Segundo o modelo *Open Systems Interconnection* (OSI) resulta:

Tabela 5 – Modelo OSI

| Camada | Protocolo |
|---|---|
| Aplicação | HTTP, HTTPS, SMTP, DNS, ARP, SNMP, SSL, Telnet, SSH, TLS |
| Transporte | TCP, UDP |
| Rede | IP (IPv4, Ipv6), ARP, ICMP |
| Ligação Lógica | Ethernet, PPP, PPPoE |
| Física | Modem, RJ11,RJ45 |

### 3.2.8 Suporte para Wi-Fi

O suporte para Wi-Fi, previsto nas características gerais, é mais adequado par UPS. A utilização e implementação deste suporte apenas fará sentido para o mercado de UPS, uma vez que a fraca segurança das redes Wi-Fi colocam em causa a sua utilização em CIB.

Com mais de dez milhões de placas de interface vendidas, a norma IEEE 802.11b - mais conhecida pela designação Wi-Fi (*wireless fidelity*) - transformou-se num padrão muito popular no início do século XXI. No entanto, as especificações 802.11b são insuficientes para assegurar uma boa interoperabilidade entre produtos. Este aspecto é da responsabilidade da *Wireless Ethernet Compatibility Alliance* (WECA), que é dona da marca de interoperabilidade Wi-Fi e em relação à qual assegura a certificação e a promoção. Mesmo assim, um grande número de empresas ainda continua renitente em adoptar este padrão devido às questões de segurança associadas às redes Wi-Fi internas.

#### 3.2.8.1 Segurança

Normalmente, são propostas três técnicas de segurança: (*i*) através do identificador de rede; (*ii*) através de senha; e (*iii*) através da restrição de acesso por verificação do endereço MAC. Estas técnicas não utilizam qualquer tipo de encriptação e uma simples escuta passiva permite quebrar a protecção. Isto é bastante fácil e pode ser efectuado mesmo à distância se forem utilizadas antenas direccionais [22].

O primeiro protocolo de segurança adoptado no âmbito das redes sem fios que conferiu no nível de ligação lógica um patamar de segurança semelhante ao das redes por cabo foi o *Wired Equivalent Privacy* (WEP).

Este protocolo, muito usado ainda hoje, utiliza o algoritmo RC4 para encriptar os pacotes que são trocados numa rede sem fio e, assim, tentar garantir confidencialidade aos dados de cada utilizador. Além disso, utiliza-se também a CRC-32 que é uma função de detecção de erros que ao fazer o "*checksum*" de uma mensagem enviada gera um ICV (*Integrity Check Value*) que deve ser conferido pelo

receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho [21].

Os principais defeitos do protocolo de segurança *Wired Equivalent Privacy* são:

- a dimensão do vector de iniciação é demasiado curta;
- a união do vector de iniciação e da chave de encriptação não é boa;
- o mecanismo de encriptação RC4 apresenta chaves fracas.

Os dois primeiros defeitos permitem a desencriptação dos pacotes sem conhecer a chave de encriptação. As chaves fracas do RC4 permitem chegar à chave de encriptação - para isso, basta "escutar" o tráfego durante tempo suficiente. Existem, assim, vários pontos fracos para atacar que são explorados pelos *software*s de *cracking* (Aisnort e Wepcrack, entre outros) disponíveis na *Web*. O *WEP* possui ainda outra falha de peso - o sistema de autenticação por pacotes. Como se baseia numa assinatura do pacote por segmentação linear, é fácil forjar um pacote forjado partindo de um pacote encriptado e bem formado [22].

Um outro protocolo de segurança existente no âmbito das redes Wi-Fi é o WPA (*Wi-Fi Protected Access* ). É um padrão internacional para aplicações que usam comunicações sem fio. O seu propósito é aumentar o nível de segurança das redes actuais e futuras. WPA é uma solução que pretende ultrapassar as vulnerabilidades conhecidas do seu antecessor WEP e inclui já algumas características do protocolo 802.11i (que estava em desenvolvimento quando o WPA foi lançado). Este protocolo também utiliza o algoritmo RC4, porém agora com algumas melhorias em relação ao WEP. Estes melhoramentos incluem:

- 802.1x / *Extensible Authentication Protocol* (EAP) que prevê a autenticação do utilizador. Este padrão é composto por três elementos:
- O solicitante – o utilizador ou cliente que quer ser autenticado.
- Um servidor de autenticação – um sistema de autenticação.

- O objecto que dá a autenticação – um dispositivo que age como intermediário entre o solicitante e o servidor de autenticação. Normalmente esse dispositivo é o ponto de acesso – Acess Point (AP);

- *Temporal Key Integrity Protocol* (TKIP) é um protocolo derivado do 802.11i que tenta resolver as vulnerabilidades conhecidas do WEP na área de encriptação de dados. Especificamente, o TKIP conserta a falha de segurança da reutilização de chaves que acontece no WEP. É composto por três tipos de componentes:

    - Uma chave de 128 b que é compartilhada tanto pelo cliente como pelo ponto de acesso.

    - O endereço MAC do dispositivo cliente.

    - Um vector de iniciação de 48 b que descreve o número de sequência de um pacote. Esta combinação garante que os vários clientes usam chaves diferentes;

- Um vector de iniciação maior (48 b contra os 24 b usados no WEP) para reduzir as hipóteses de reutilizar as mesmas chaves de encriptação;

- Algoritmo de verificação de integridade de mensagens para ajudar a proteger a integridade dos dados transmitidos.

Alguns dos benefícios do WPA em relação ao WEP são:

- Aplicação de um forte controlo de acesso à rede através de autenticação mútua (entre clientes e AP);

- Adopção de chaves dinâmicas no TKIP para estabelecer uma melhor gestão de chaves (evitando chaves duplicadas);

- Reforço da integridade dos dados através do algoritmo de verificação de integridade de mensagens.

Problemas encontrados no WPA:

- Apesar de ser mais difícil, persiste o risco de quebra da encriptação do TKIP;

Actualmente a prova da confiabilidade e robustez do WPA permanece uma incógnita [28].

Entretanto surgiu o WPA2, com o objectivo de conferir maior segurança às redes *wireless* do que as oferecidas pelos protocolos WEP e WPA. Os protocolos WEP e WPA utilizam o algoritmo RC4 para encriptação de dados que oferecia o nível de segurança adequado. Um novo algoritmo foi usado para o protocolo WPA2, o *Advanced Encryption Standard* (AES). A especificação deste protocolo inclui muitas características do IEEE 802, são elas:

- *Temporal Key Integrity Protocol* (*TKIP)*: para manter o suporte a dispositivos mais antigos, o 802.11i escolheu o TKIP para padrão de encriptação (o mesmo do WPA);

- *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (*CCMP)*: o 802.11i inclui outro padrão conhecido como AES-CCMP, que requer uma implementação em *hardware* para operar;

- *Wireless Robust Authentication Protocol (WRAP)*: este protocolo utiliza o algoritmo de encriptação AES em conjunto com outro modo de operação para lidar com encriptação e integridade;

- Integridade da mensagem: é aplicado um algoritmo de integridade dos dados robusto - *Michael Message Integrity Check* (igual ao WPA);

- Autenticação mútua: o 802.11i usa o 802.1X/EAP para autenticação do utilizador (igual ao WPA); O protocolo 802.11i tem todas as vantagens descritas no WPA.

Adicionalmente, o WPA2 oferece uma encriptação forte através da implementação do AES. A única desvantagem conhecida deste protocolo é a

necessidade de actualizar o *hardware*, para que o algoritmo AES possa ser implementado [28].

#### 3.2.8.2 *Hardware*

Para dotar o servidor da capacidade de se ligar a uma rede Wi-Fi, é necessário, além de instalar módulos de expansão para rede Wi-Fi (*software*), adicionar uma placa com um receptor Wi-Fi.

Figura 60 – Adaptador de rede PCI com tecnologia Wi-Fi

### 3.2.9 Aplicações Disponibilizadas

Ao nível das aplicações, o servidor deverá disponibilizar um serviço sobre HTTP que garanta a monitorização e controlo em tempo real sobre os componentes do sistema que supervisiona. Em termos gerais, deverá disponibilizar páginas compatíveis com a maioria dos navegadores *Web* disponíveis no mercado actual e fazer uso das mais recentes tecnologias que permitam implementar uma troca de dados em tempo real de forma segura.

Deverá, assim, possuir as seguintes características:

- Sistema de autenticação dos utilizadores com vários níveis de acesso;
- Gestão de utilizadores;
- Gestão de grupos de utilizadores;
- Registo de acessos ao servidor;
- Gestão de grupos de equipamentos (adição/remoção de equipamentos);

- Acesso a valores de medidas por componente;
- Histórico de medidas e alarmes dos vários componentes;
- Sinóptico configurável;
- Sinóptico por CIB;
- Actualizações de valores em tempo real;
- Monitorização e controlo de rectificadores, baterias e de entradas/saídas auxiliares;
- Definição de parâmetros de funcionamento para cada componente.

Além destas características, o servidor deverá igualmente dispor de *software* que faça a recepção de dados, tanto por RS-232 como por SNMP, tratar a informação e armazená-la numa base de dados. Esta base de dados poderá ser acedida pela aplicação *Web*, via Telnet (ligação local e remota) e SNMP. Deverá incluir *software* que faça a monitorização dos valores que recebe e lance alertas através de correio electrónico, *traps* de SNMP, SMS e/ou *pager* para o operador responsável pelo equipamento e/ou administrador do sistema.

Poderá ter, como módulos opcionais, *software* para análise dos dados guardados na base de dados (análise de desempenho, análise de carga/descarga das baterias, *etc.*) assim como guias interactivos de resolução de problemas que possam vir a afectar um CIB.

A arquitectura a adoptar pelo sistema deverá ser modular de forma a torná-lo versátil e expansível em termos de características. Deverá ser fácil e simples adaptar o sistema às necessidades e requisitos de cada cliente, evitando alterar o código fonte do núcleo do servidor. Esta característica trará ainda vantagens no que diz respeito ao desenvolvimento futuro do sistema e à integração com sistemas mais vastos de monitorização integrada de equipamentos distribuídos.

# 4 Descrição do Suporte Físico

Para facilitar a compreensão plena do objectivo desta aplicação, será importante conhecer as características dos módulos de *hardware* que compõem um CIB. Segue-se então, uma descrição introdutória desse mesmo *hardware* utilizado.

## 4.1 Bastidor CIB

O armário técnico CIB constitui, em associação com uma bateria um sistema de alimentação ininterrupto, permitindo aos equipamentos ligados obter uma alimentação CC (Corrente Contínua), insensível às diversas perturbações que possam ocorrer na rede de alimentação. Este bastidor reúne como principais características, uma topologia modular e de fácil acesso.


Figura 61 – Bastidor Efapower CIB S 48/34 x 34

## 4.2 Módulo PSM

O Módulo PSM é uma unidade de comando e supervisão, que permite a monitorização remota do CIB no local, utilizando uma porta de comunicações RS-232 e uma linha telefónica (PSTN ou GSM).

O microprocessador incluído nesta unidade assegura as seguintes funções:

- Gestão e supervisão geral do sistema;
- Geração de alarmes e sinalizações por relés;
- Possibilidade de obter no *display* medidas analógicas:
- Correntes (à entrada do rectificador ; carga/descarga bateria; de saída);
- Tensões (à entrada *bypass*; Bateria; à saída do inversor);
- Temperatura (Bateria; Ambiente);
- Frequência (Entrada; Inversor);
- Potência (Saída em kW e kVA);
- Factor de pico (corrente de entrada e de saída);
- Cálculo do tempo de autonomia da bateria em função da carga;
- Disparo de Protecções Eléctricas;
- Vigilância do estado dos fusíveis e disjuntores;
- Vigilância da qualidade da tensão de saída;
- Comando do interruptor estático;
- Possibilidade de desligar a UPS por telecomando (para situações de emergência);

- Memorização dos últimos 255 eventos incluindo a data e hora [5].

Figura 62 – Módulo PSM

### 4.2.1 Menus Disponíveis

Tendo em conta que aplicação deverá desempenhar as mesmas funções que podem ser desempenhadas através de um teclado, é importante referir quais os dados disponibilizados no ecrã de cristais líquidos existente no PSM e a sua respectiva disposição.


Figura 63 – PSM vista inicial

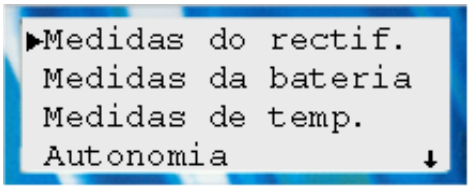


Figura 64 – PSM Menu Principal

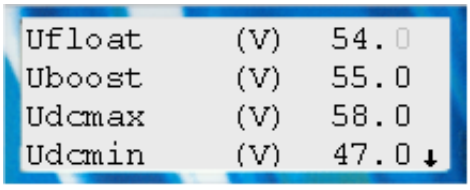


Figura 65 – PSM Menu Edição de Parâmetros

De acordo com as necessidades dos clientes, algumas secções do menu podem ser desactivadas. Caso não existam limitações, são estes os elementos disponíveis através do ecrã:

- Medidas do rectificador;
- Medidas da bateria;
- Medidas de temperatura;
- Autonomia;
- Parâmetros;
- Alarmes actuais;
- Histórico;
- Apagar histórico;
- Ver estados;
- Comandos;
- Configuração.

## 4.3 Módulo SNMP

O módulo SNMP que permite disponibilizar os dados da unidade de supervisão (PSM) anteriormente descrita através de uma rede IP. No caso de equipamentos sem PSM, o adaptador SNMP dispõe de entradas e saídas livres que podem ser utilizadas para ligar directamente ao equipamento a monitorar. O adaptador baseia-se num microprocessador de 32 b Motorola ColdFire, com capacidade de processamento suficiente para assegurar a encriptação e permitir a monitorização de forma segura (através da criação de uma VPN sobre IPsec). Cada alimentador reporta a um servido central em ambiente Linux, onde é executada uma aplicação que se encarrega de

comunicar com os alimentadores. Esta comunicação é feita a pedido ou, em caso de alarme, é automaticamente desencadeada pelo alimentador.

Nessa aplicação, é possível monitorizar e configurar as funcionalidades do sistema (medidas, alarmes, parâmetros, *logger*, *etc.*). Uma base de dados instalada no servidor disponibiliza informações sobre cada alimentador (alterações, intervenções, *etc.*) e sobre os grupos de utilizadores autorizados a ligar-se ao sistema, com diferentes níveis de permissões e diferentes grupos de equipamentos aos quais têm acesso. O servidor central inclui uma aplicação servidora que assegura ainda a geração de páginas *Web* para permitir o acesso de aplicações cliente (navegadores *Web*) a partir de qualquer computador.

A utilização do protocolo SNMP, que é um protocolo "aberto", permite (caso o cliente o deseje) integrar esta monitorização num sistema mais vasto de gestão central como, por exemplo, o HP OpenView. Neste caso, a EFACEC S.E. disponibilizará a MIB que descreve o sistema para que seja integrada no sistema de supervisão escolhido pelo cliente. [6]

Figura 66 – Módulo SNMP

# 5 Descrição da Aplicação Desenvolvida

## 5.1 Módulos do Sistema

O sistema desenvolvido é construído sobre um servidor de base de dados, que comporta a base de dados onde se armazenam os dados sobre os equipamentos e dos utilizadores, e um *webserver*, onde se alojará a aplicação *Web* que é o *front-end* do utilizador, e alguns módulos adicionais de interacção com os equipamentos remotos e de gestão de alarmes.

Os dados serão actualizados periodicamente na base de dados, nomeadamente informações de histórico de alarmes, estado de equipamentos, dados e configurações de equipamentos, *etc.,* através do módulo de comunicações. A aplicação servidora obterá os dados directamente da base de dados e, em casos específicos, directamente dos equipamentos.

Foram assim definidos quatro grandes módulos:

- Módulo de Interface com o Utilizador;
- Módulo de Comunicações;
- Módulo da Base de Dados;
- Módulo de Gestão de Alarmes.

O Módulo de Interface com o Utilizador é, como já foi referido, o *front-end* que comunica com o navegador do utilizador e que lhe permite interagir com os sistemas de alimentação distribuídos. Para este efeito foi utilizado um servidor http, que pode ser instalado em qualquer PC, onde foi alojada a aplicação *Web* desenvolvida.

O Módulo de Comunicações é responsável por estabelecer as ligações com os equipamentos distribuídos, seja na Ethernet, seja via modem analógico.

O Módulo da Base de Dados é, essencialmente, um servidor de base de dados que contém a base de dados da informação relativa aos equipamentos, utilizadores, alarmes e configurações.

O Módulo de Gestão de Alarmes é o módulo responsável pela recepção de alarmes de equipamentos e actualização da base de dados de histórico de alarmes.

A arquitectura da aplicação apresenta os seguintes módulos:

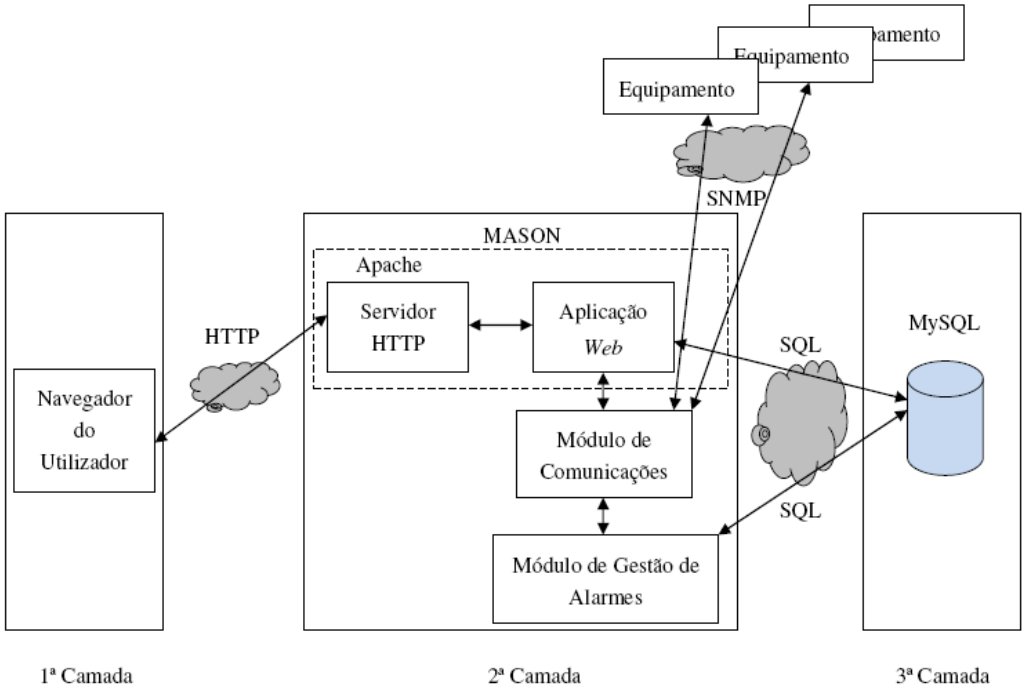


Figura 67 – Interligação entre módulos do sistema

## 5.2 Desenvolvimento do *Software*

### 5.2.1 Tecnologias Utilizadas

Nesta secção são abordadas as tecnologias utilizadas neste projecto, nomeadamente, as linguagens de programação utilizadas ao longo do projecto desenvolvido.

#### 5.2.1.1 HTML

HTML (*HyperText Markup Language)*, que significa *Linguagem de Anotação de Hipertexto*, é uma linguagem de anotação utilizada para produzir páginas *Web* – documentos HTML – que são interpretados pelos navegadores. A tecnologia é fruto do "casamento" dos padrões HyTime e SGML [53].

#### 5.2.1.2 JavaScript

JavaScript é uma linguagem de programação baseada em guiões criada pela Netscape em 1995, que a princípio se chamava LiveScript, para atender, principalmente, as seguintes necessidades:

- Validação de formulários no lado cliente (navegador *Web*);
- Interacção com a página.

É uma linguagem de *scripting*, com uma sintaxe semelhante à do Java, mas totalmente diferente no conceito e no uso:

- Não tem tipos pré-definidos de variáveis;
- É interpretada, ao invés de compilada;
- Possui óptimas ferramentas padrão para listagens (característica comum a todas as linguagens de *scripting*);
- Oferece bom suporte a expressões regulares (característica comum a todas as linguagens de *scripting*).

A união do Javascript com o *Cascading Style Sheets* (CSS) é conhecida como *Dynamic HTML* (DHTML), que permite modificar dinamicamente os estilos dos elementos das páginas *Web* [54].

#### 5.2.1.3 AJAX

O AJAX (acrónimo em língua inglesa de *Asynchronous Javascript And XML*) consiste no uso combinado de Javascript e XML por parte dos navegadores para tornar as

páginas mais interactivas ao utilizador, fazendo uso de pedidos assíncronos de informação. O AJAX não é somente um novo modelo, é também uma contribuição importante para a construção de aplicações *Web* mais dinâmicas e criativas. O AJAX ao integrar duas tecnologia oferece novas funcionalidades. O AJAX incorpora no seu modelo:

- Apresentação baseada em padrões, usando XHTML e CSS;
- Exposição e interacção dinâmica usando o DOM;
- Intercâmbio e manipulação de dados usando XML e XSLT;
- Recuperação assíncrona de dados usando o objecto XMLHttpRequest;
- JavaScript unindo todos estes componentes.

O modelo clássico de aplicação *Web* trabalha assim: o utilizador gera na interface (navegador *Web*) um evento que desencadeia um pedido HTTP ao servidor HTTP. O servidor encaminha o pedido para a aplicação Web em causa, a aplicação realiza o processamento recuperando dados, realizando cálculos, conversando com outras aplicações — e retorna uma página HTML com o resultado para o cliente.

A maior vantagem das aplicações AJAX é que elas executam no âmbito do próprio navegador *Web*. Então, para se estar habilitado a executar aplicações AJAX, basta possuir algum dos navegadores modernos, ou seja, lançados após 2001 (Mozilla Firefox, Internet Explorer 5+, Opera, Konqueror e Safari) [55].

#### 5.2.1.4 Perl

Perl é uma linguagem de programação estável e multiplataforma, usada em aplicações de missão crítica em todos os sectores, sendo destacado o seu uso no desenvolvimento de aplicações *Web* de todos os tipos. A origem do Perl remonta ao *shell scripting*, Awk e linguagem C. Está disponível para praticamente todos os sistemas operativos, sendo contudo usado com maior frequência em sistemas Unix e compatíveis.

É especialmente versátil no processamento de cadeias de caracteres (*strings*), manipulação de texto e no *pattern matching* implementado através de expressões regulares. Além disso, dada a sua simplicidade, permite tempos de desenvolvimento curtos [56].

#### 5.2.1.5 Mason

HTML::Mason, ou apenas Mason, é o nome de um ambiente integrado de desenvolvimento e execução de aplicações *Web* escrito em Perl e distribuído pela *Comprehensive Perl Archive Network* (CPAN). As funcionalidades deste ambiente permitem efectuar o desenvolvimento de aplicações *Web* com conteúdo dinâmico e de grande afluência, tais como jornais, bases de dados e *sites* de comércio electrónico. Alguns *sites* populares como o Amazon.com ou o de.licio.us são suportados pela arquitectura e funcionalidades do ambiente Mason.

O estilo do Mason é semelhante ao StoryServer e até ao PHP, mas o Mason faz uso do Perl como linguagem de controlo, podendo por isso utilizar quase todos os módulos desenvolvidos em Perl e disponibilizados no CPAN.

O Mason pode ser instalado como um módulo no servidor *Web* da Apache [57].

As peças que compõem o Mason são conhecidas como “componentes”. Um componente é uma mistura de código HTML, Perl e de comandos especiais do Mason. Enquanto os componentes de nível superior (ou *top-level*) representam as páginas *Web* os componentes mais pequenos que retornam tipicamente pedaços de código HTML e destinam-se a ser integrados em componentes de níveis superiores.

Uma arquitectura orientada aos objectos facilita a manutenção deste tipo de *sites*. A alteração de um componente partilhado reflecte-se em todos os componentes de níveis superiores e, por sua vez, a alteração propaga-se a todo o *site*.

A arquitectura Mason permite ao programador dividir o *site* em elementos de programação, módulos e componentes de *design,* assim como incluir excertos de código Perl no meio de código HTML para gerar páginas de conteúdo dinâmico.

O Mason funciona interceptando pedidos HTTP *Requests* e redireccionando-os para os seus componentes. O Mason compila o componente, executa-o e devolve o *output* ao cliente.

A título ilustrativo apresenta-se o seguinte componente de Mason:

```
% my $noun = 'World';
Hello <% $noun %>!
How are ya?
```

do qual resulta o:

```
Hello World!
How are ya?
```

Neste componente pode-se ver mistura entre código HTML e elementos Mason. O divisor '%' na primeira linha avisa o Mason que se segue uma linha de código em Perl. Já a linha abaixo com a etiqueta <% … %> embebida coloca o resultado da execução do Perl na página de HTML [58].

#### 5.2.1.6 Servidor HTTP da Apache

O Servidor de HTTP Apache, mais conhecido como servidor Apache, é um servidor *Web* que contribuiu para o rápido crescimento inicial da WWW (*World Wide Web*). O Apache é desenvolvido e mantido por uma comunidade aberta de programadores sob supervisão da Apache Software Foundation. Está disponível para uma grande gama de sistemas operativos incluindo o Unix, o FreeBSD, o Linux, Solaris, Novell NetWare, Mac OS X, Microsoft Windows, *etc.* É fornecido sob a licença da Apache e é caracterizado como um *software* livre.

O Apache suporta uma grande variedade de funcionalidades, muitas implementadas como módulos compilados que permitem aumentar as funcionalidades de base. Estas funcionalidades podem passar pela inclusão de programas do lado do servidor tais como as interfaces mod_perl, mod_python e PHP. Disponibiliza vários módulos de autenticação nomeadamente os módulos como

SSL e TLS. Suporta ainda módulos de compressão tais como os módulos externos mod_gzip que, implementados, permitem a redução das páginas *Web* disponibilizadas [59].

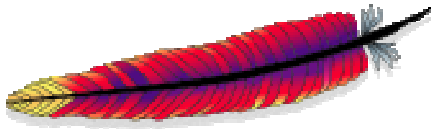

Figura 68 – Logótipo do Servidor HTTP Apache

#### 5.2.1.7 MySQL

O MySQL é um sistema de gestão de base de dados (SGBD) que utiliza a linguagem SQL (*Structured Query Language* - Linguagem de Consulta Estruturada) para interagir com os clientes. É actualmente um dos servidores de bases de dados mais populares, com mais de 10 milhões de instalações pelo mundo. Tem como principais características:

- Portabilidade (suporta praticamente qualquer plataforma actual);
- Compatibilidade (existem controladores ODBC, JDBC e .NET e módulos de interface para diversas linguagens de programação, como Delphi, Java, C/C++, Python, Perl, PHP. ASP e Ruby);
- Excelente desempenho e estabilidade;
- Pouco exigente quanto a recursos de *hardware*;
- Facilidade de uso;
- É um *software* livre;
- Suporta vários tipos de tabelas (MyISAM, InnoDB, *etc.*);
- Implementa controlo transaccional;
- Permite a definição de *Triggers*;
- Permite a definição de *Stored Procedures* e *Functions*;

- Replicação facilmente configurável.

## 5.3 Descrição de Módulos

### 5.3.1 Módulo de Comunicações

A aplicação *Web* necessita de comunicar com os equipamentos para obter dados relativos ao seu funcionamento. Existem duas formas de comunicar com os equipamentos remotos:

- Via Ethernet (rede):
- Via Modem (linha telefónica).

Se o equipamento CIB dispuser de um módulo Efapower SNMP, este disponibiliza uma interface Ethernet com um endereço IP atribuído. Desta forma, é possível obter dados do equipamento através de pedidos de SNMP directos.

Se, por outro lado, o equipamento não dispuser de um módulo Efapower SNMP ou apenas dispuser de um modem analógico, a ligação deverá ser efectuada através do modem. Este modem analógico estará ligado directamente ao controlador do CIB (PSM, MiniPSM ou MicroPSM). Os dados serão obtidos através de uma ligação série criada entre o modem do equipamento e o modem da plataforma do servidor, que permite aceder à memória do equipamento.

Desta forma, a lógica adoptada foi a seguinte:

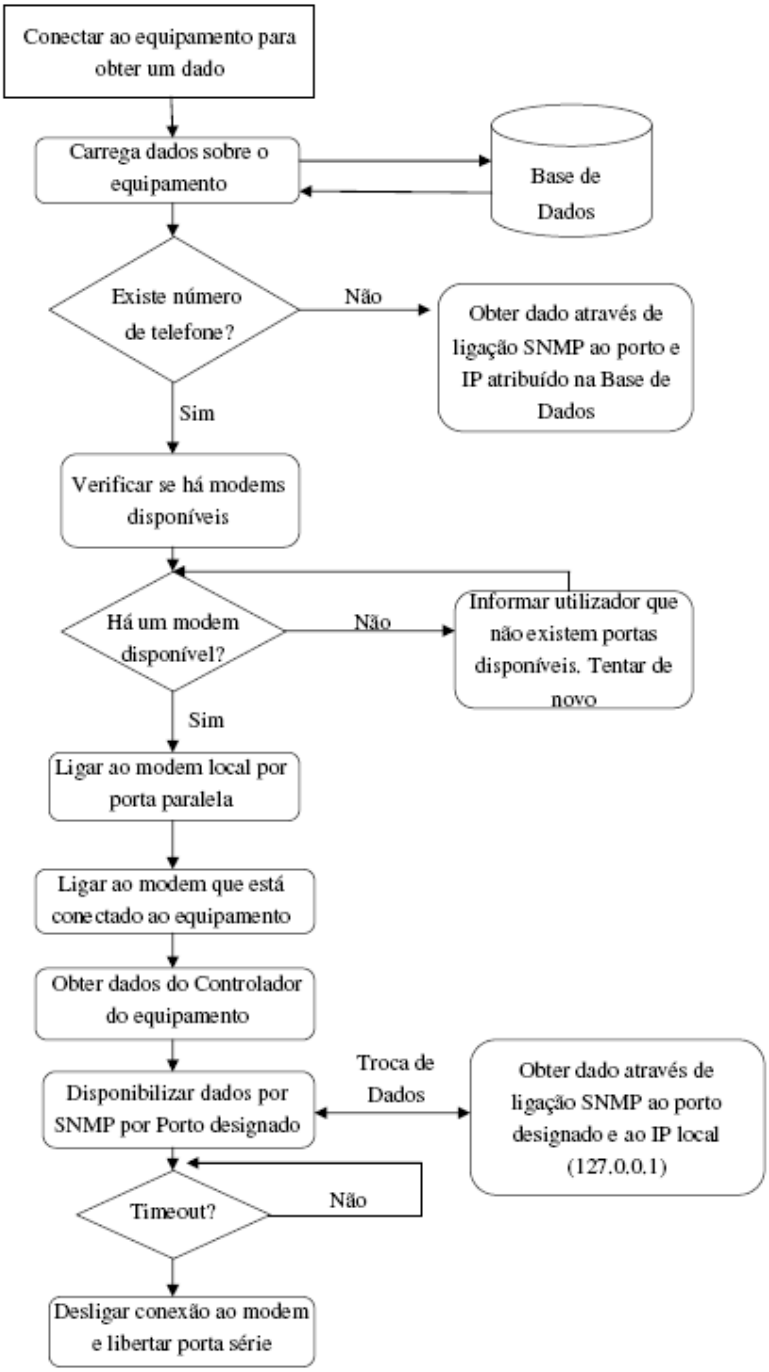


Figura 69 - Lógica do módulo de comunicação

Sempre que dados são requisitados a um equipamento, seja para a base de dados, gestão de alarmes ou refrescamento dos dados da aplicação *Web*, é efectuado um pedido de SNMP para o OID específico, para o IP do equipamento e para o porto de SNMP designado.

Para tal, é utilizado um *script* de Perl que engloba vários tipos de pedidos de OID diferentes e executa um pedido de SNMP. Este *script* denominado de *deamon.pl* utiliza o módulo Net::SNMP disponível nas bibliotecas do CPAN. Este módulo permite, através de um endereço IP, porto e OID fazer uma chamada específica de SNMP. É possível obter e enviar dados para o equipamento utilizando este protocolo de comunicação específico.

O deamon.pl disponibiliza um conjunto de funções tais como:

```
my $funcs = {doSNMPget => \&doSNMPget,
             doSNMPwalk => \&doSNMPwalk,
             getSoftwareVersion => \&getSoftwareVersion,
             getClientName => \&getClientName,
             getControllerSN=> \&getControllerSN,
             getBatName => \&getBatName,
             getBatNum => \&getBatNum,
             getBatNumElem => \&getBatNumElem,
             getBatAutonomy => \&getBatAutonomy,
             getBatStatusString => \&getBatStatusString,
             getBatRegimeCarga => \&getBatRegimeCarga,
             getBatMeasures => \&getBatMeasures,
             getBatParameters => \&getBatParameters,
             getSerial => \&getSerial,
             getPropDCNominal => \&getPropDCNominal,
             getManufName => \&getManufName,
             getManufDate => \&getManufDate,
             getPropTriphase => \&getPropTriphase,
             getUdc => \&getUdc,
             getIdc => \&getIdc,
             getIbat => \&getIbat,
             getRectName => \&getRectName,
             getRectMax => \&getRectMax,
             getRectType => \&getRectType,
             getRectAddr => \&getRectAddr,
             getRectStatus => \&getRectStatus,
             getRectCommand => \&getRectCommand,
             setRectCommand => \&setRectCommand,
             getRectIout => \&getRectIout,
             getRectVout => \&getRectVout,
             getRectTemp => \&getRectTemp,
             getRectVin => \&getRectVin,
             getConnTime => \&getConnTime,
             getAlrms => \&getAlrms,
             getPropFrequency => \&getPropFrequency,
             getControllerName => \&getControllerName,
             getEPROMVersion => \&getEPROMVersion,
             getSNMPAgentV => \&getSNMPAgentV,
             getStatusMenu => \&getStatusMenu,
             getStatusText => \&getStatusText,
             getStatusTextToggles =>
\&getStatusTextToggles,
```

```
            getCommandsMenu => \&getCommandsMenu,
            getCmdText => \&getCmdText,
            getCmdTextToggles => \&getCmdTextToggles,
            getParameterMenu => \&getParameterMenu,
          AlarmsResend => \&AlarmsResend,
          HistReset => \&HistReset,
          DetectRect => \&DetectRect,
          ResetRect => \&ResetRect,
          setVal => \&setVal,
          BatTest => \&BatTest,
          MaxTime => \&MaxTime,
          getMaxTime => \&getMaxTime,
          Voltage => \&Voltage,
          getVoltage => \&getVoltage,
          Current => \&Current,
          getCurrent => \&getCurrent,
          command => \&command,
          sendEmail => \&sendEmail,
          registTrapDaemon => \&registTrapDaemon,
          signalTrapDaemon => \&signalTrapDaemon,
          getAuxInText => \&getAuxInText,
          getAuxOutText => \&getAuxOutText,
          getAuxInValue => \&getAuxInValue,
          getAuxOutValue => \&getAuxOutValue,
          setauxout => \&setAuxOutValue,
          getConnOnline0 => \&getConnOnline0,

          };
```

Um exemplo típico de uma função que toma partido das funcionalidades disponibilizadas pelo módulo SNMP pode ser demonstrado por este trecho de código referente à obtenção de alarmes do equipamento.

```
sub getAlrms {
    my ($R, $sh) = @_;
  if ($R->{'ip'} and $R->{'community'}) {
        my $pid = fork();
        if ($pid != 0) {
                close $sh;
                return;
        } else {
                   my $res;
                   my $value;
                   $R-
>{'oid'}=".”.#.#.#.#.#.#.#.#.#.#.#";
                   my $out=(sys_SNMPget($R));
                   if ($out->{'res'} eq
"TIMEOUT") {
                        $res='nok';
                        $value='TIMEOUT';
                   } else {
                        $res='ok';
                        $value = $out-
>{'res'};
```

```
                    }
                    print $sh
Dumper({res=>$res,value=>$value,ip=>$R-
>{ip}});
                close $sh;
                exit;
        }
  } else {
        print $sh
Dumper({res=>'nok',reason=>'no ip or
community'});
  }
}
```

Neste caso, o OID foi ocultado no código por questões de segurança.

Quando o equipamento não tem atribuído um endereço IP, mas um número de telefone, este estará acessível através de um modem analógico.

Desta forma, é necessário criar uma ligação entre modems analógicos e comunicar através destes como se trate de uma ligação série. Para tal, utiliza-se um modem externo com ligação a portas série. Usando o módulo Device::Modem, disponível no CPAN, pode-se comunicar com o modem local e efectuar uma ligação ao modem do equipamento por *dial-up*. Este módulo faz uso de comandos AT (Hayes) normais de comunicação entre modems. Para que este módulo funcione, necessita de um outro, que permite controlar a ligação à porta série. Este módulo adicional que foi instalado é denominado Device::SerialPort e necessita de ser compilado especificamente para a distribuição em que é utilizado. Dado que estes módulos de Perl são construídos em C, é necessário compilar o módulo com um compilador de C. O módulo Device::SerialPort é específico para Linux e baseia-se num módulo semelhante disponível para sistemas operativos Windows denominado Win32::SerialPort.

A lógica a implementar para este sistema necessitava de prever a utilização de vários modems, de realizar o controlo sobre a ligação em curso e de ter mecanismos de segurança que permita desactivar a ligação.

Foi criada, para este efeito, uma rotina especial no módulo *deamon.pl* denominado *gestAcess* que permite determinar quais as portas série disponíveis e

atribuir uma a um novo pedido de comunicação. Este módulo verifica que utilizador está a tentar aceder a que equipamento e, no caso de não existir ainda nenhuma ligação activa para esse equipamento, executa um módulo denominado de *dial.pl* responsável por efectuar a ligação e a manter activa.

O módulo *dial.pl* recebe como parâmetros a porta série livre e o número de telefone e estabelece a ligação ao modem do equipamento remoto. Uma vez efectuada a ligação, executa um código binário desenvolvido em C e denominado *appkit* que lê os dados da memória do controlador e disponibiliza os dados num servidor de SNMP embutido. Este código foi adaptado de um código semelhante criado para o Efapower SNMP que efectuava a mesma função, ligando directamente ao equipamento através da interface série.

O *script dial.pl* retorna o novo de porto de SNMP disponibilizado pelo *appkit*, o qual deve ser usado pela aplicação para efectuar pedidos por SNMP. Desta forma, a maneira como o servidor *Web* acede aos dados (por pedidos de SNMP) não é alterada, permitindo manter-se a estrutura de comunicação.

A ligação é controlada pelo próprio processo *dial.pl* que fica activo durante a duração da comunicação. O *dial.pl* tem como função implementar um *timeout* que, uma vez terminado, desactiva o *appkit* e fecha a ligação ao modem, libertando o porto série. Cada chamada de SNMP que é efectuada incrementa o *timeout*, permitindo manter a chamada activa por períodos longos.

Em termos de lógica temos:

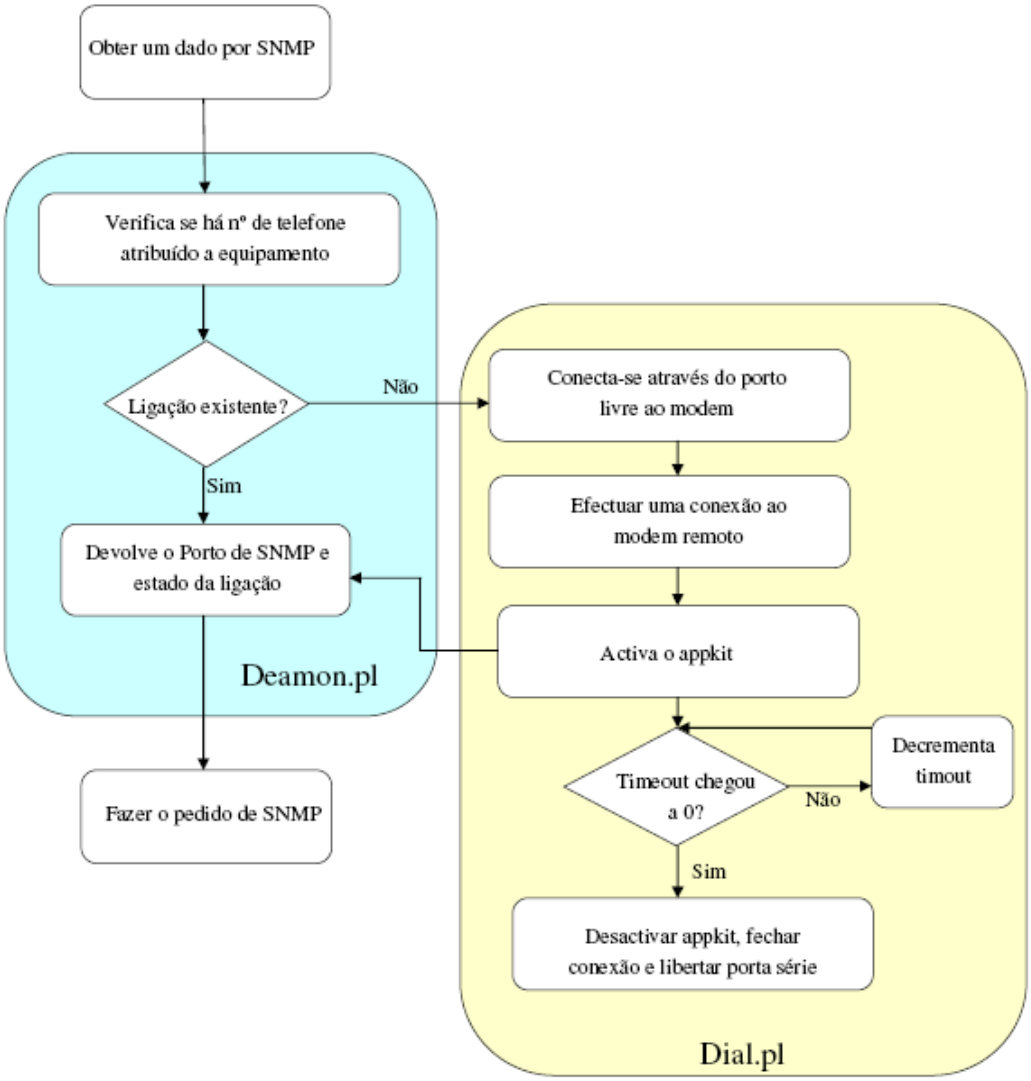


Figura 70 - Lógica de comunicação

O ficheiro de controlo e configuração tem os seguintes campos:

```
### Fields in modem.txt
#
# ttyS0|0|0|0|0|0|0
#
# 1 - Serial Port indication
# 2 - User ID
# 3 - Equipment ID
# 4 - Port assigned for SNMP Port
# 5 - PID from appkit process assigned
# 6 - State of conection
# 7 - Timeout bit
# 8 - commands for conection control
```

Um extracto do código mostra como, através de um *fork*, se lança o código *appkit* com as definições específicas necessárias para o processo, *i.e.,* a porta série a utilizar, a configuração do SNMP e o porto SNMP a ser criado.

```
my $comma;
my $pidd = fork();
die "unable to fork: $!" unless
defined($pidd);
if (!$pidd) {  # child
    #exec('command...');
    #die "unable to exec: $!";
  $comma = "/bin/appkit -p $at_port -c $commu
-s $port";
  system ($comma);
}else{
# parent continues here, pid of child is in
$pidd
$pidd = $pidd+1;

# continue processing in the parent after
child is done
#begin timeout of connection
```

O *appkit*, após ser lançado, lê através da porta série os dados directamente do controlador do CIB. A limitação imposta pela configuração do modem do lado do CIB (uma taxa de transmissão máxima de 4800 b/s) faz com que o *appkit* só disponibilize os dados ao fim de cerca de 4 min. Após estes 4 min, em que o *appkit* carrega para o servidor o total conteúdo da MIB do PSM, os dados são enviados à aplicação *Web*, sendo efectuadas apenas actualizações constantes de determinados valores, tais como estados e medidas.

Este excerto de código de um dos módulos da aplicação *Web* demonstra como se processa uma chamada à função *gestAcess* que controla as ligações aos modems.

```
<%def .cibSysPage2>
<%perl>
my @arr = $arg->{'sth'}->fetchrow_array;
my $res;
my $rest;
my $onl;

#online?
if ($arr[15] eq "0")
{

$res = serverCall("127.0.0.1",
5000,{op=>'doSNMPget',ip=>$arr[3],community=>$arg-
```

```
>{'community'},oid=>'.#.#.#.#.#.#.#.#.#.#.#.#',port=>$ar
r[8]});

}else{

$rest = serverCall("127.0.0.1", 5000,
{op=>'gestAcess',iduser=>$arg->{session}-
>{'uid'},idequip=>$arg->{'id'}});

$res = serverCall("127.0.0.1",
5000,{op=>'doSNMPget',ip=>"127.0.0.1",community=>$arg-
>{'community'},oid=>'.#.#.#.#.#.#.#.#.#.#.#.#',port=>$re
st->{'nport'}});

}
if($res->{'res'} eq "0")
{
$onl="0";
}else{
$onl="1";
}
```

De forma a obter um determinado dado por SNMP, determina-se se o equipamento tem um número de telefone atribuído. Caso tenha, é chamada a função *gestAcess*.

```
$rest = serverCall("127.0.0.1", 5000,
{op=>'gestAcess',iduser=>$arg->{session}-
>{'uid'},idequip=>$arg->{'id'}});
```

O output ( $rest->{‘nport’} ) é o porto SNMP ao qual a aplicação *Web* se deve ligar. O IP para o qual deverá ligar é 127.0.0.1, ou seja, o *localhost*.

```
$res = serverCall("127.0.0.1",
5000,{op=>'doSNMPget',ip=>"127.0.0.1",community=>$arg-
>{'community'},oid=>'.#.#.#.#.#.#.#.#.#.#.#.#',port=>$re
st->{'nport'}});
```

### 5.3.2 Módulo da Base de Dados

A base de dados construída comporta a seguinte informação:

- Dados de configuração do equipamento *host* (onde é executado o gestor);
- Dados de configuração do servidor *Web*;
- Dados sobre os equipamentos;

- Dados sobre os alarmes (histórico);
- Dados sobre as falhas de equipamentos ou de rede;
- Dados sobre os acessos dos utilizadores;
- Dados sobre os utilizadores (grupos, *etc.*);
- Dados dinâmicos guardados a pedido do utilizador;

**Dados de Configuração do *Host***

Guarda definições importantes tais como o endereço MAC, endereço IP, sistema operativo, informações adicionais que possam ser necessárias.

**Dados de configuração do servidor *Web***

Guarda configuração de correio electrónico para envio de alertas, nome de utilizador, servidor e/ou número de telemóvel para envio de alerta SMS, definição de estilo para cada tipo de utilizador, *etc.*)

**Dados sobre equipamentos**

Quais os equipamentos activos, endereços IP, informações úteis sobre a MIB, grupo a que pertencem, versão da MIB, protocolo SNMP suportado, nome do equipamento, tipo de equipamento, data da última actualização do estado, alarmes activos, *etc.*;

Esta tabela será constantemente actualizada pelo gestor de alarmes e pelos acessos do utilizador a um equipamento específico.

**Dados sobre alarmes (histórico)**

Guarda a informação de alarmes detectada pelo gestor de alarmes:

- Tipo de alarme;
- Tipo de equipamento;

- Equipamento;
- Data de início;
- Data de fim.

**Dados sobre falhas de equipamentos ou de rede**

Guarda dados relativos a períodos de tempo em que um equipamento esteve *offline* ou incontactável.

**Dados sobre os utilizadores**

Guarda os dados dos utilizadores que incluem:

- Identificador;
- Nome de Utilizador;
- Nome Completo;
- *Password*;
- Endereço de *email*;
- Telefone;
- Empresa;
- Identificação;
- Cargo na empresa;
- Tipo de função no sistema;
- Informação adicional;
- Idioma a usar no sistema.

**Dados sobre os acesso dos utilizadores**

Os utilizadores que acederem ao sistema ficam com o seu IP e data de acesso registados, mesmo que não tenham sido autorizados a aceder ao sistema.

Em termos de implementação a base de dados foi criada no MySQL. Este servidor de base de dados apresenta várias vantagens, nomeadamente o facto de ser *open source*. A base de dados criada é constituída pelas seguintes tabelas:

**alarm_equipment**

Tabela com informação relativa a alarmes recebidos ou recolhidos dos diversos equipamentos do sistema. É a partir desta tabela que o histórico de alarmes e tabela de alarmes activos são construídas.

*hid* - identificação única

*date_start* - data de início do alarme

*date_stop* - data de fim de alarme

*state* - estado do alarme (ON/OFF)

*eid* - *id* do equipamento

*aid* - *id* do alarme

*ackno* - *flag* de indicação se o alarme foi aceite pelo operador (YES/NO)

*oper* - nome do operador que aceitou o alarme

*date_time_ack* - data e hora da aceitação do alarme

*meth* - método utilizado para enviar o alerta (aplicação *Web*, SMS, *email*, *etc*.)

**alarm_table**

Tabela com todos os alarmes que o equipamento dispõe no seu sistema.

*aid* - identificação única

*indexe* - índice do alarme no equipamento

*alarm_text* - texto do alarme

*description* - descrição do alarme

*date* - data da recolha do alarme

*priority* - prioridade associada ao alarme

*alid* - identificação de configuração de alarme

*eid* - *id* do equipamento

*active* - *flag* de indicação se o alarme está activo

**alert_config**

Tabela com configuração tipo para configurar cada tipo de alarme

*alid* - identificação única

*tipo* - tipo de alarme

*email* - *flag* de indicação se envia *email* para utilizadores

*SMS* - *flag* de indicação se envia SMS para utilizadores

*temp_email* - Modelo de *email*

*temp_SMS* - *template* de SMS

*Oper* – envio de SMS e *email* para operadores

*Admin* – envio de SMS e *email* para administradores de sistema

**asso_cont**

Tabela que associa cada alarme à sua respectiva configuração

*conid* - identificação única

*alid* - identificação de configuração de alarmes

*uid* - identificação do utilizador associado ao tipo de alarme

*email* - endereço de *email* de utilizador (utilizado no caso de não haver um utilizador associado ao endereço de *email*)

*SMS* - número de SMS de utilizador (utilizado no caso de não haver um utilizador associado ao número de telemóvel)

*no_user_flag* - *flag* que indica se existe um utilizador associado

**asso_equip**

Tabela que associa cada equipamento a um grupo ou conjunto de grupos de equipamentos.

*gid* - identificação do grupo

*name* - nome do equipamento associado

*eid* - identificação do equipamento

**asso_users**

Tabela que associa cada utilizador a um grupo ou conjunto de grupos de utilizadores.

*gid* - identificação do grupo

*name* - nome do utilizador associado

*uid* - identificação do utilizador associado

**equipgroups**

Tabela que contém informação acerca dos grupos de equipamentos.

*gid* - identificação do grupo

*pgid* - identificação da posição

*location* - localização do grupo

*extratext* - texto descritivo

**equipment**

Tabela que contém informação acerca dos equipamentos.

*eid* - identificação única

*name* - nome do equipamento

*location* - localização do equipamento

*ip* - IP associado ao equipamento (caso não seja atribuído será 0)

*tagid* - identificação única para Scatex

*foward* - *flag* de envio de *emails*

*gatex* - *flag* de envio de dados para Scatex

*email* - *email* associado ao equipamento

*port* - porto associado ao SNMP

*alid* - identificação do tipo de configuração de alerta

*alarm_flag* - indicação de alarme activo em equipamento

*online_flag* - *flag* que indica se *software* está *online* ou não

*type* - tipo de equipamento

*communications* - tipo de interface que utiliza (Ethernet ou Modem)

*community* - indicação de configuração de community SNMP

*phone* - número de telefone associado (se nenhum associado é 0)

*disa_alarms* - *flag* de desactivação de alarmes

**loglevels**

Tabela com informação acerca dos níveis de acesso e erros associados.

*loglevel* - identificação única

*name* - texto para identificação do tipo de erro

**logs**

Tabela com informação acerca dos acessos ao servidor.

*eid* - identificação de equipamento

*uid* - identificação de utilizador

*loglevel* - nível de alarme

*logstr* - estado do histórico

*date* - data do histórico

*ip* - IP do acesso ao servidor

**privs**

Tabela com informação acerca dos níveis de acesso de cada utilizador.

*guid* - identificação do grupo de utilizador

*geid* - identificação do grupo de equipamentos

*access* - nível de acesso

*privid* - identificação das sessão

**sessions**

Tabela com informação acerca da sessão.

*id* - identificação única

*length* - tamanho da sessão

*a_session* - sessão

**usergroups**

Tabela com informação acerca dos grupos de utilizadores.

*gid* - identificação de grupo

*pgid* - identificação processo

*extratext* - texto extra

**users**

Tabela com informação relativa aos utilizadores.

*uid* – identificação única

*username* – nome de utilizador

*nome* – nome completo do utilizador

*priv* – nível de acesso

*password* – *password* do utilizador

*email* – endereço de correio electrónico

*telefone* – número de telefone do utilizador

*empresa* – nome da empresa do utilizador

*identificação* – identificação profissional

*funcao* – função desempenhada na empresa

*obs* – campo para observações do utilizador

*pref_lang* – indicação para língua preferida para utilizador.

Para aceder a esta informação, dentro do código Perl podemos utilizar código como o exemplificado no excerto abaixo:

```
$dbh = DBI->connect("DBI:mysql:$database:localhost",
      $dbuser, $dbpass );
my $sth = $arg->{'dbh'}->prepare("select * from
equipgroups where location='". $arg->{'nome'} ."'");
$sth->execute();
```

Este pedido específico permite ler todos os campos da tabela *equipgroups* em que o campo *location* tenha um valor semelhante à variável *$arg->{'nome'}.*

### 5.3.3 Módulo da Aplicação *Web*

O módulo da Aplicação *Web* tem uma importância especial dado é a face visível do sistema.

Para se desenvolver a aplicação *Web* de interface com o utilizador optou-se por se utilizar um servidor de HTTP, nomeadamente o Apache HTTP Server. A aplicação *Web* foi desenvolvida dentro de uma pasta *chroot* por questões de portabilidade e segurança em sistemas Unix[iii].

Para o desenvolvimento e disponibilização da aplicação *Web* foi utilizado o ambiente Mason, que permite um desenvolvimento modular, rápido e seguro, tirando partido das potencialidades dos módulos de Perl pré-existentes, tais como o CPAN.

[iii] A operação *chroot* no sistema Unix muda a raiz de ficheiros do sistema para todos os processos em execução. Esta operação permite proteger os ficheiros originais do sistema contra eventuais ataques ao sistema [60].

#### 5.3.3.1 Ambiente Mason

O ambiente de desenvolvimento Mason para a disponibilização da aplicação Web utiliza um ficheiro (*autohandler*) sempre que é pedida uma página ao servidor *Web*, *i.e.,* qualquer pedido efectuado para o servidor *Web* é encaminhado, obrigatoriamente, para este ficheiro. Este modo de funcionamento permite controlar todos os aspectos da navegação de um utilizador através do servidor *Web* e das aplicações *Web* aí instaladas.

Tem-se acesso a toda a informação acerca da sessão de cada utilizador (identidade, linguagem pré-definida, base de dados, *etc.)* que é guardada num objecto de sessão e que permite passar argumentos entre diferentes módulos das aplicações *Web*. Os diferentes módulos que compõem a aplicação *Web* são construídos independentemente e trocam informação do objecto dessa sessão. Este esquema de construção permite uma manutenção e torna a construção de novas funcionalidades do servidor *Web* muito fácil.

Esta arquitectura permite a criação de páginas de conteúdo dinâmico recorrendo a linguagens tais como o HTML, JavaScript e Perl, permitindo uma construção de páginas dinâmicas e interactivas com o utilizador assim como garante um acesso fácil à base de dados (servidor de bases de dados utilizado é MySQL). Uma outra tecnologia que foi incorporada neste desenvolvimento foi o AJAX. O AJAX permite o refrescamento assíncrono dos dados da página que é mostrada ao utilizador, de forma não incomodativa (evita o refrescamento da página toda), reduzindo o fluxo de informação para o mínimo necessário.

#### 5.3.3.2 Aplicação de AJAX

A estrutura do AJAX obedece a regras pré-determinadas. O AJAX realiza pedidos http assíncronos. Tradicionalmente, quando se pretende obter informação de uma base de dados ou de um ficheiro existente na plataforma do servidor ou enviar informação de um cliente para um servidor, necessitamos de incluir um formulário HTML na página *Web* e utilizar o método GET ou POST para interagir com a aplicação. Neste contexto, o utilizador tem de pressionar na tecla de *submit* para

enviar a informação que preencheu no formulário e esperar pela nova página devolvida pelo servidor com os resultados, desejados.

Como cada vez o cliente submete informação o servidor retorna uma página nova, as aplicações tradicionais funcionam mais lentamente e tendem a ser menos *user-friendly*. Com o AJAX, os excertos de JavaScript comunicam directamente com o servidor, através do objecto de XMLHttpRequest do Javascript. Estes pedidos são feitos ao servidor e são recebidas respostas sem haver a necessidade de recarregar toda a página. O utilizador continua a visualizar a mesma página que, no entanto, foi actualizada de forma transparente, *i.e.,* não se apercebeu da execução dos *scripts* pedindo dados ou recebendo dados do servidor [61].

O ponto fulcral do AJAX são os objectos XMLHttpRequest. Diferentes navegadores usam métodos diferentes para criar os objectos de XMLHttpRequest:

- O Internet Explorer usa o ActiveXObject;
- Outros navegadores usam os objectos de JavaScript chamados XMLHttpRequest;

Para criar este objecto e lidar com diferentes navegadores, utiliza-se uma estrutura de controlo de fluxo do tipo *try* e *catch*.

```
function GetXmlHttpObject()
{
var xmlHttp=null;
try
{
// Firefox, Opera 8.0+, Safari
xmlHttp=new XMLHttpRequest();
browser=2;
}
catch (e)
{
// Internet Explorer
try
{
xmlHttp=new
ActiveXObject("MSXML2.XMLHTTP.4.0");
browser=1;
}
catch (e)
{
```

```
xmlHttp=new
ActiveXObject("Microsoft.XMLHTT");
browser=1;
}
}
return xmlHttp;
}
```

Os dados enviados pelo servidor podem ser recebidos através da propriedade *responseText*.

```
function stateChanged()
{
if(xmlHttp.readyState==4)
{
inter1=self.setInterval(function(){ajaxfunctio
on()},3000);
if(xmlHttp.responseText==null)
{
}
else
{
if(response==xmlHttp.responseText)
{
i++;
}
else
{
response=xmlHttp.responseText;
document.getElementById("txtHint").innerHTML=
xmlHttp.responseText;
}
}
}
return xmlHttp;
}
```

Para enviar um *request* para o servidor, usaram-se os métodos *open()* e *send().*

O método *open()* recebe três argumentos:

- primeiro argumento define que método se utiliza-se para enviar o *request* (GET ou POST);
- o segundo argumento especifica o URL do *script* do lado do servidor.;
- o terceiro argumento especifica que o *request* deve ser tratado de forma assíncrona.

O método *send()* envia o *request* para o servidor.

```
function ajaxfunction(str)
{
xmlHttp=null;
xmlHttp=GetXmlHttpObject();
self.clearInterval(inter1);
if(xmlHttp==null)
{
alert(\"Your browser does not support
AJAX!\");
return;
}
if(browser==2)
{
xmlHttp.open("GET","../cgi-bin/cib.cgi?inf
",true);
xmlHttp.setRequestHeader("If-Modified-
Since","Sat, 1 Jan 2000 00:00:00 GMT");
xmlHttp.onreadystatechange=stateChanged;
xmlHttp.send(null);
}
if(browser==1)
{
xmlHttp.onreadystatechange=stateChanged;
xmlHttp.open("GET","../cgi-bin/cib.cgi?inf
",true);
xmlHttp.setRequestHeader("If-Modified-
Since","Sat, 1 Jan 2000 00:00:00 GMT");
xmlHttp.send(null);
}
}
```

Nesta função é introduzida a linha *xmlHttp.setRequestHeader()* para obrigar o navegador Internet Explorer a actualizar a página após a recepção dos dados do servidor. Assim compara o cabeçalho da página corrente e actualiza-a sempre que houver uma alteração. De notar a linha *self.setInterval(function(){ajaxfunction()},3000)* que auto-executa a função *ajaxfunction* a cada 3 s. Esta função é responsável por enviar o pedido de actualização de dados para o servidor.

#### 5.3.3.3 Sinóptico

A utilização de um sinóptico é outra parte importante do servidor *Web*. Para tal foi utilizado um ficheiro desenvolvido em *Scalable Vector Graphics* (SVG). Este ficheiro é utilizado noutros *software*s de monitorização e controlo de equipamentos tais como o Efapower SNMP servidor *Web* e o Efacon, foi igualmente adoptado e integrado na visualização dos equipamentos. Contém um *script* de Javascript que permite a

reconstrução da imagem de SVG de acordo com os dados recebidos pela aplicação *Web*.

Tendo em que conta que o objectivo é a criação de uma plataforma adaptável de construção de sinópticos, foram criadas algumas sintaxes especiais. As sintaxes criadas permitem que, somente através da edição do ficheiro SVG, se possa configurar todo o sistema. A partir do sinóptico, é possível definir de quais e de que tipos de endereços determinado texto ou cor de objecto depende.

| | *id* | *label* |
|---|---|---|
| **Definição de Objectos** | **OBJS** | @(obj1)* (obj…) *(objN)! |
| **Definição de Propriedades (para 3 condições)** | **prop_**(objecto) | @(I/O entrada saída)/(resultado se 1)/( resultado se 0)<br>@(I/O entrada saída)/(resultado se 1)/( resultado se 0)<br>@(I/O entrada saída)/(resultado se 1)/( resultado se 0) |
| **Subtracção** | **caption_SUB_**(numero caption1)_( numero caption2) | ---------- |
| **Definição de Etiquetas** | **caption_**(numero) | @(endereço medida) |
| **Definição de Objecto que muda a cor** | (objs) **_fill** | |
| **Definição de Objecto que comuta caso endereço seja 0** | (objs) **_obj0** | |
| **Definição de Objecto que comuta caso endereço seja 1** | (objs) _obj1 | |

Figura 71 - Síntese de edição do Sinóptico

Para promover a comunicação entre a aplicação e o Javascript foi necessário implementar uma sintaxe própria, que permitisse informar quais os endereços dos estados e das medidas necessários ao sinóptico. Construiu-se então uma trama com uma estrutura adequada que se apresenta na figura seguinte.

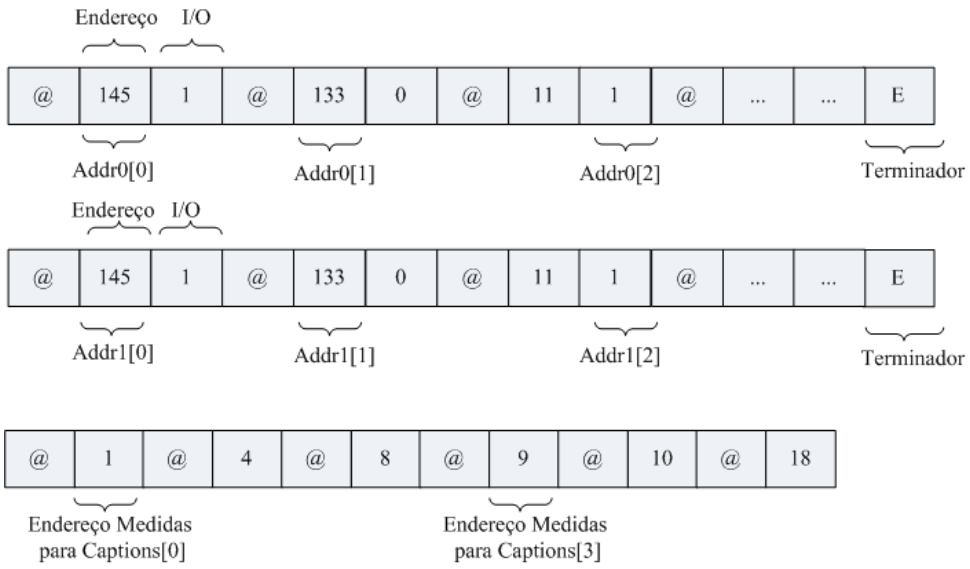


Figura 72 – Estrutura da mensagem

### 5.3.4 Módulo de Gestão de Alarmes

Este módulo é responsável pelas recepções de alarmes dos equipamentos, actualização da base de dados e consulta dos vários equipamentos para fazer o levantamento do estado de cada equipamento monitorizado.

O modo de operação foi estruturado em duas modalidades distintas:

- conectar por SNMP aos equipamentos;
- conectar por modem aos equipamentos.

#### 5.3.4.1 Recepção de SNMP *Traps*

Para implementar um sistema de recepção de *traps* por SNMP, foi necessário estabelecer um sistema de recepção de *heartbeats.* Um *heartbeat* é um *trap* SNMP com um OID específico que é enviado periodicamente pelo equipamento. Este sinalizador periódico indica que o equipamento está activo (*online*). A não recepção deste *trap* específico por parte de um determinado equipamento levará a originar um alarme específico no sistema, alertando que o equipamento deixou de estar *online*.

A tabela de *heartbeats* é uma tabela com a identificação dos equipamentos, data da última recepção de *heartbeat* e *timeout* regressivo. Por cada nova recepção de um *heartbeat,* esta tabela é actualizada com nova data e restauro do valor inicial de *timeout*. Um processo lançado em paralelo é responsável por decrementar todos os *timeout* de cada equipamento e verificar se algum chegou a 0. Quando um *timeout* chega a zero, é lançado um alarme que irá ser adicionado aos alarmes activos e ao histórico do Efapower Webserver.

Desta forma é possível aos utilizadores do sistema saber que um dos equipamentos deixou de responder e actuar em conformidade com o previsto.

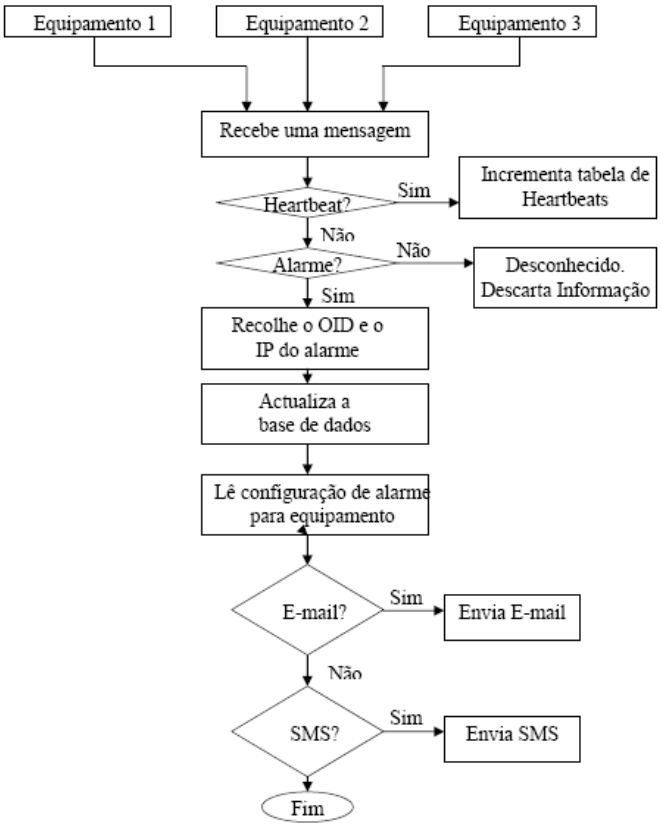


Figura 73 – Lógica de recepção de alarmes

#### 5.3.4.2 *Polling* aos Equipamentos

De forma a actualizar a base de dados e obter a lista dos alarmes activos dos equipamentos monitorizados, pode ser implementado um *polling* periódico.

Este processo é lançado periodicamente, percorre e liga-se a todos os equipamentos existentes na base de dados. Obtém os alarmes activos, determina se o equipamento está *online* ou não e actualiza a tabela de alarmes específica de cada equipamento.

Começa por consultar a base de dados para obter o endereço IP ou número de telefone associado a cada equipamento e verificar se possui uma tabela com alarmes actualizada. Para cada equipamento lança um conjunto de pedidos de dados por SNMP. Após a recepção desses dados, actualiza a base de dados.

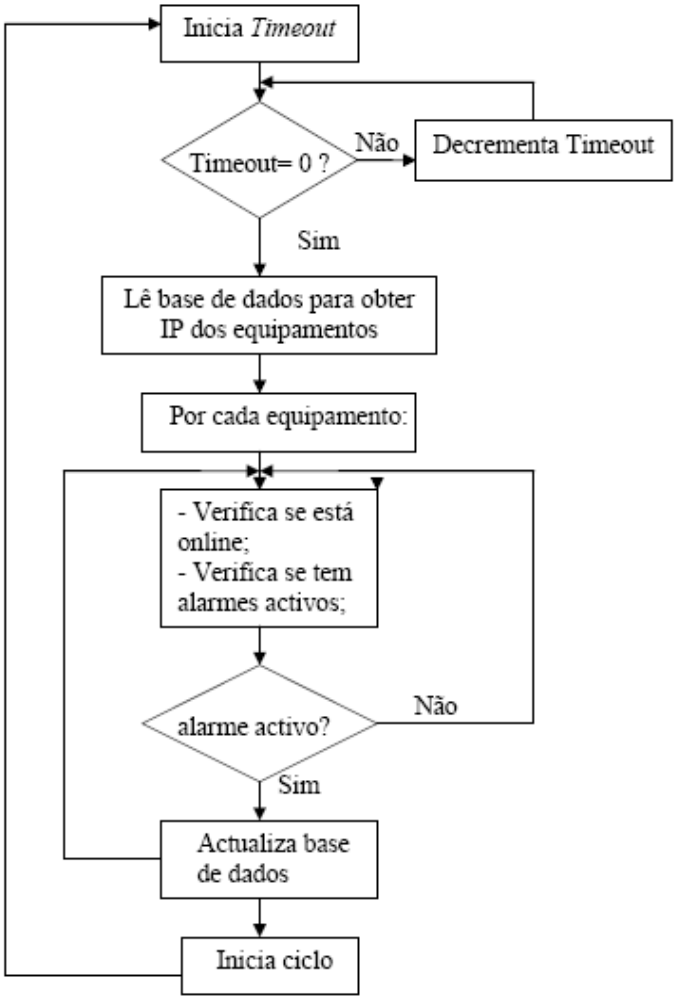


Figura 74 – Lógica de funcionamento do processo de *polling*

# 6 Funcionalidades do Projecto

O projecto apresenta funcionalidades ao nível da monitorização e controlo de múltiplos equipamentos distribuídos geograficamente. O desenvolvimento levado a cabo durante o período de estágio na EFACEC permitiu desenvolver um conjunto de funcionalidades que tornam este produto extremamente atractivo para a empresa.

## 6.1 Autenticação

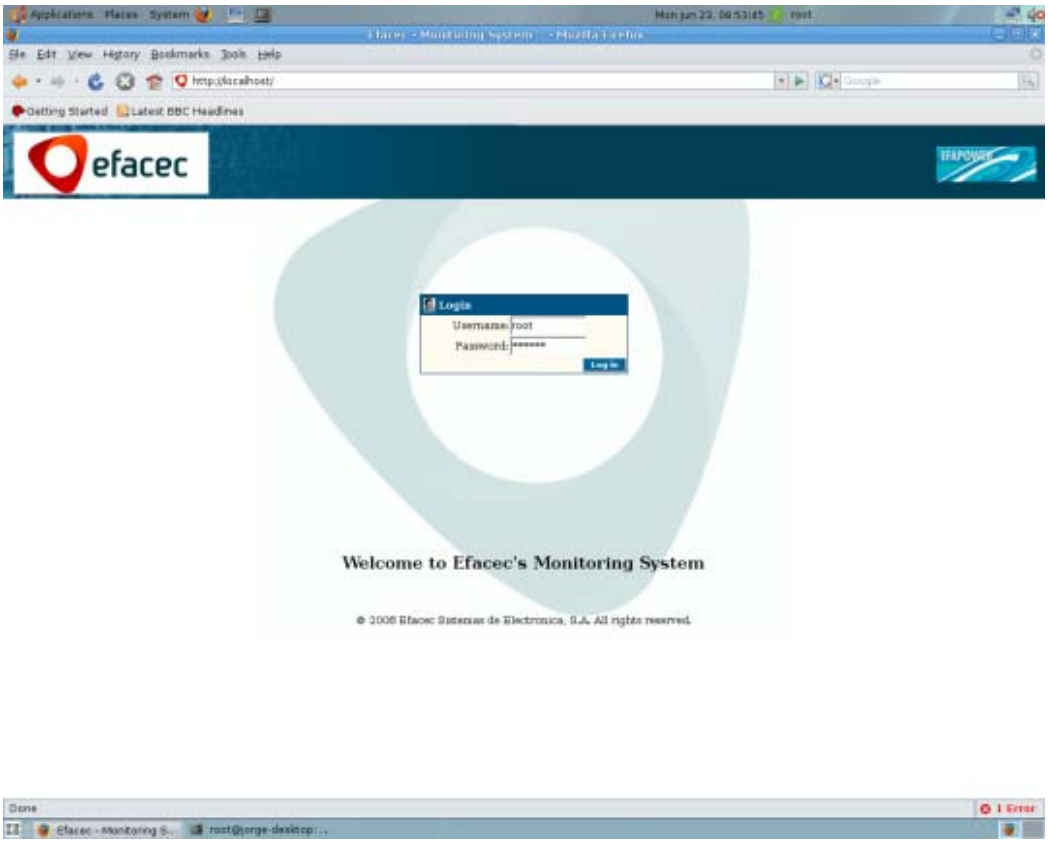


Figura 75 – Autenticação

A página inicial é uma página de autenticação dos utilizadores, sendo necessário inserir o *username* e a *password*. Estes dados são então comparados com os existentes na base de dados e, caso sejam coincidentes, é dado acesso ao conteúdo da aplicação *Web*.

## 6.2 Página de Boas-Vindas

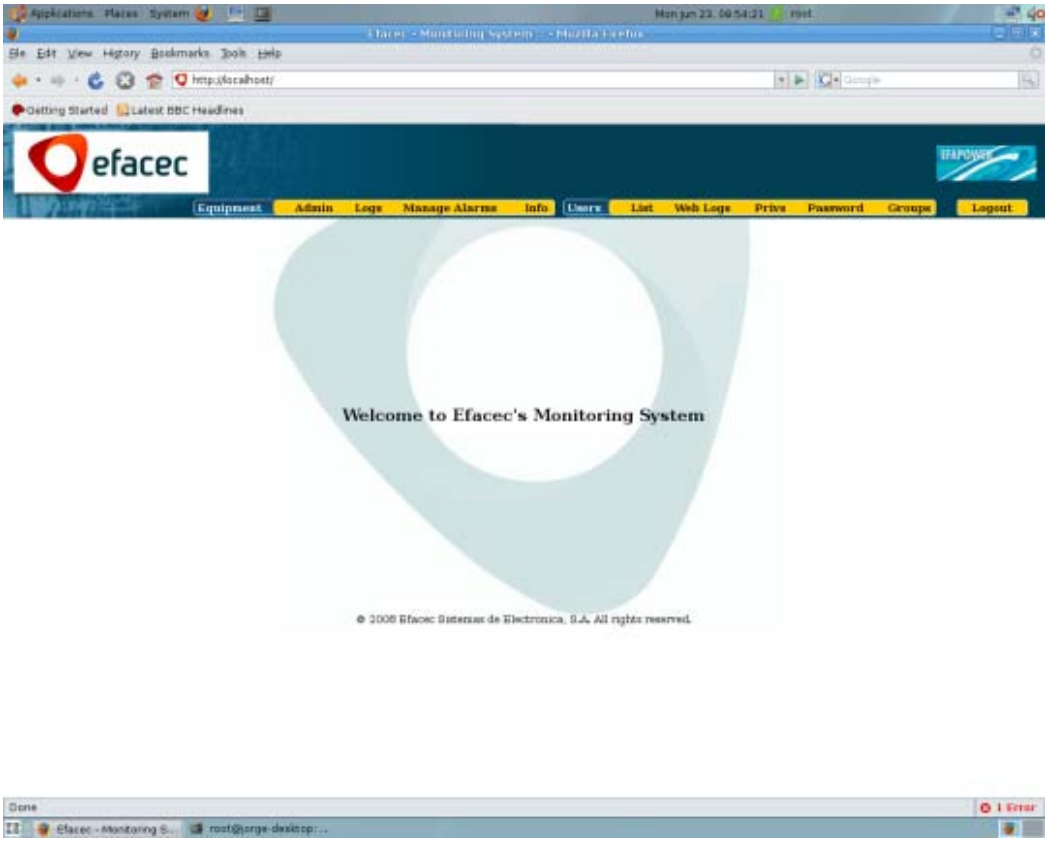


Figura 76 - Página principal/Boas-vindas

Após efectuar a autenticação, o utilizador entra numa página em que são visíveis a amarelo os menus disponíveis no Efapower WebServer. Os menus encontram-se divididos em menus relativos aos equipamentos e aos utilizadores.

Nos menus relativos aos equipamentos encontram-se o menu de Administração (*Admin*), Histórico (*Logs*), Gestão de alarmes (*Manage Alarms*) e Informação (*Info*).

Nos menus relativos aos utilizadores encontram-se o menu de Listagem de utilizadores (*List*), Listagem de acessos (*Web Logs*), Níveis de acesso (*Privs*), senha (*Password*) e Grupos (*Groups*).

## 6.3 Menu de Administração

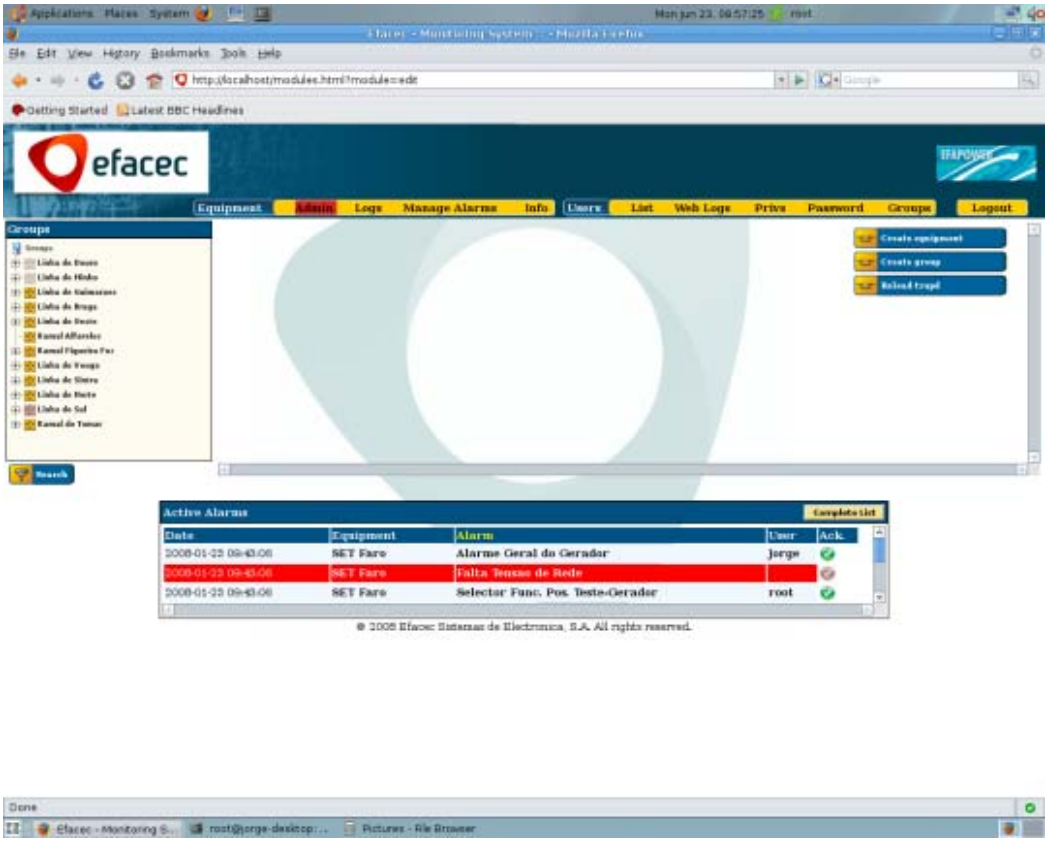


Figura 77 - Menu de Administração

O menu de administração apresenta uma organização de página diferente. Destacam-se uma estrutura (ou árvore) de equipamentos do sistema do lado esquerdo uma caixa, em baixo, com os alarmes activos no momento e um *frame* interior com opções relativas ao menu.

O *frame* da esquerda apresenta os grupos de equipamentos que podem ser expandidos para se aceder aos respectivos equipamentos. Clicando sobre o grupo, o conjunto de equipamentos que o constitui surge. Funciona de uma maneira semelhante ao Explorer do Windows, tornando-se muito intuitivo.

Se um equipamento do grupo tiver um alarme activo, o símbolo do grupo pisca em vermelho. Clicando sobre esse grupo, o símbolo que se encontra junto ao equipamento com alarme activo também pisca em vermelho. As actualizações são constantes, periódicas e imperceptíveis ao utilizador.


Figura 78 - Estrutura de equipamentos

O outro elemento com actualizações constantes e periódica é a tabela de alarmes activos no sistema.


Figura 79 - Tabela de alarmes activos

Esta tabela apresenta os alarmes activos, em que equipamentos estão a ocorrer e a data da ocorrência. O lado direito da tabela apresenta uma coluna destinada à aceitação do alarme por parte do utilizador. Este sistema serve, essencialmente, para informar os restantes utilizadores que tenham acesso ao sistema que o tratamento deste alarme foi assumido por um técnico, que passa a ser responsável por eventuais manutenções no equipamento ou desencadear algum protocolo.

Os botões a verde indicam que o alarme foi aceite e por quem. Os botões que piscam em vermelho indicam que o alarme necessita ainda de ser atribuído a alguém.

Clicando sobre qualquer das colunas é possível reorganizar a informação que consta da tabela. Clicando sobre o botão Lista Completa (*Complete List*) o utilizador é redireccionado para o histórico de alarmes completo do sistema. Clicando sobre

qualquer dos equipamentos ou utilizadores é redireccionado para informação detalhada acerca dos mesmos.

O menu central apresenta as seguintes opções:

- Criar Equipamento (*Create equipment*);
- Criar Grupo (*Create group*);
- Reiniciar Trapd (*Reload Trapd*).

### 6.3.1 Criação de um Equipamento

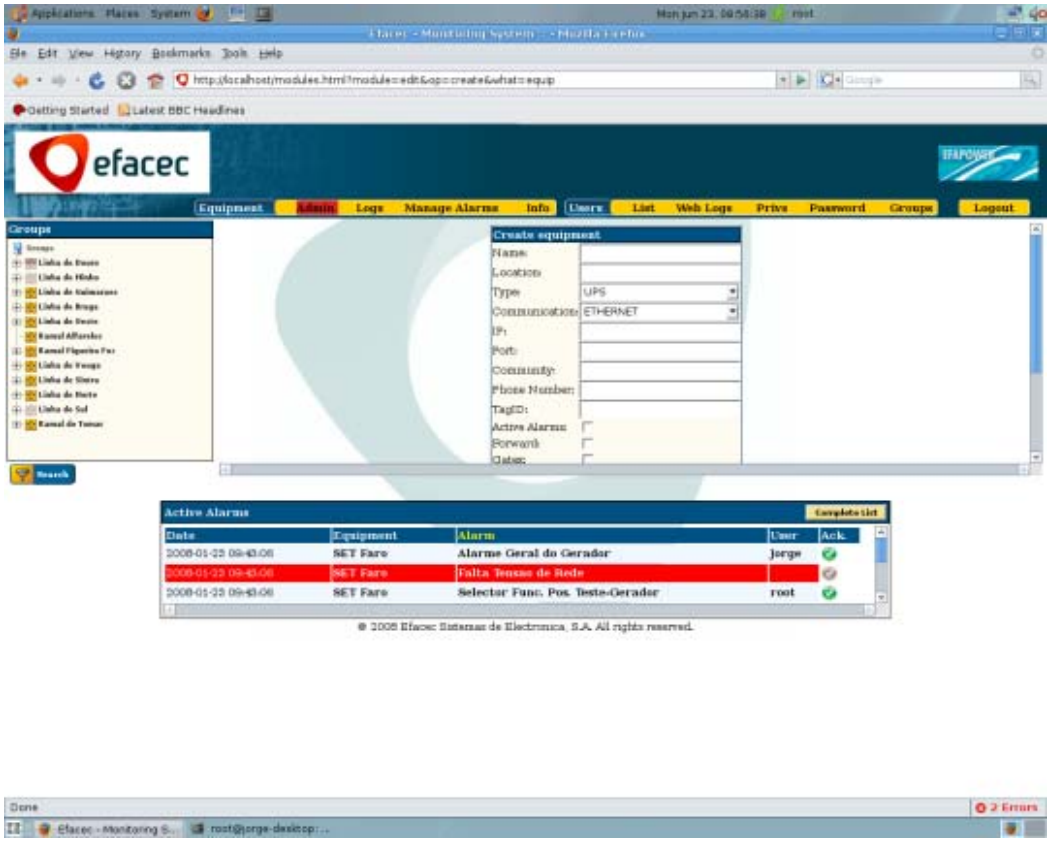


Figura 80 - Criação de um equipamento

O menu criar equipamento permite adicionar um novo equipamento no sistema. Podemos adicionar manualmente o equipamento em todos os campos ou carregar um equipamento semelhante e modificar apenas os dados diferentes.

Os campos disponibilizados são:

- Nome (*Name*) – Nome do equipamento;
- Localização (*Location*) – Localização do equipamento;
- Tipo (T*ype*) – Tipo de equipamento (UPS/CIB);
- Comunicação (*Communication*) – Interface de comunicação (Modem/Ethernet);
- IP – Endereço de rede;
- Porto (*Port*) – Porta de SNMP que a aplicação *Web* deve contactar;
- Comunidade (*Community*) – Tipo de configuração do SNMP;
- Número de telefone (*Phone Number*) – Número de telefone associado ao equipamento;
- TagID – Etiqueta de identificação para o sistema Scatex;
- Alarmes Activos (*Active Alarmes*) – *Flag* que indica se os alarmes do equipamento são ignorados ou não;
- Envio (*Foward*) – *Flag* para o envio de alarmes;
- Gatex – *Flag* para activar envio de alarmes para o Scatex;
- *Email* – *Email* associado ao equipamento;

Abaixo desta tabela de entrada de dados, encontra-se uma segunda tabela onde estão definidos os alarmes do equipamento, nível de prioridade de cada equipamento, tipo de configuração de alarme associada a esse tipo de alarme, descrição e data do último refrescamento da informação relativa a alarmes no equipamento.

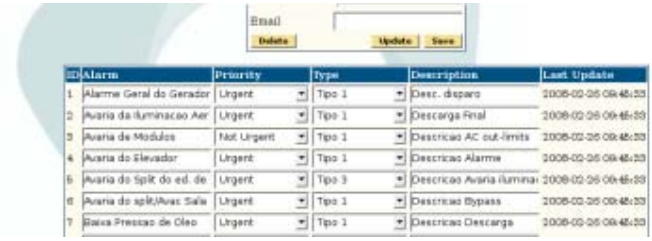


Figura 81 - Tabela de alarmes do equipamento

Os dados que constam nesta tabela podem ser carregados manualmente ou a partir de outro equipamento idêntico.

### 6.3.2 Edição de um Equipamento

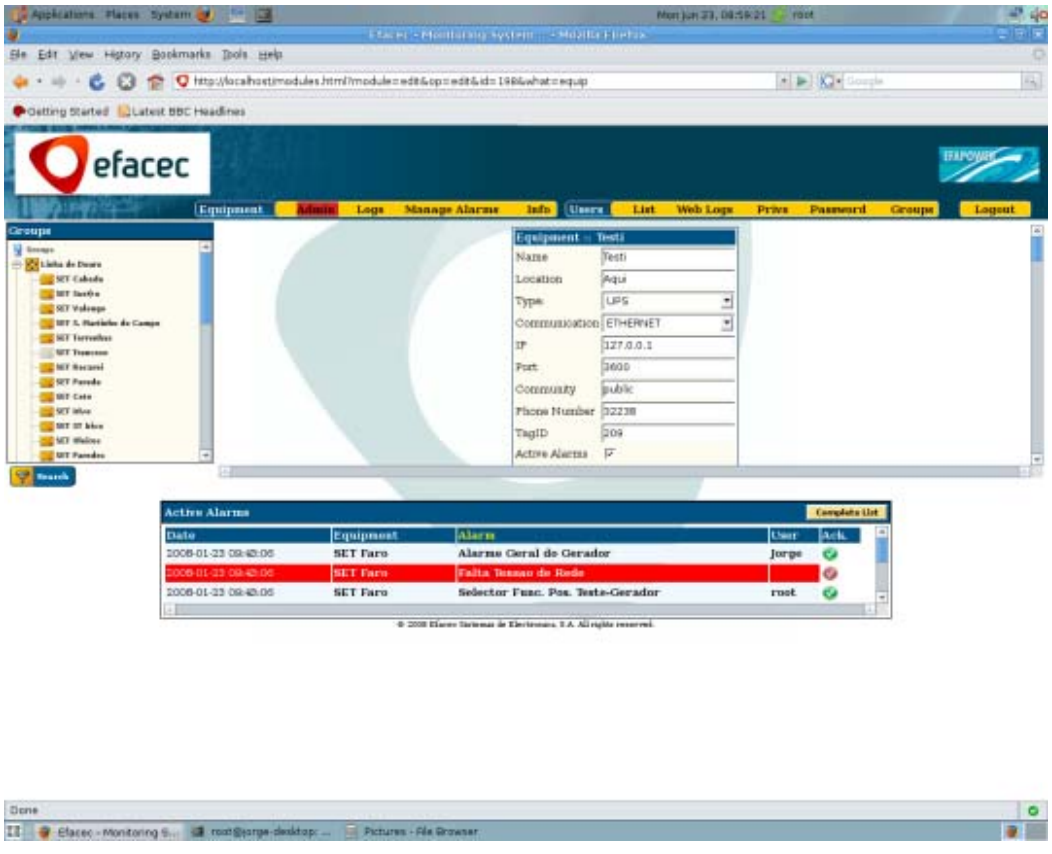


Figura 82 - Edição de equipamento

No menu de edição de equipamento é possível, clicando sobre o equipamento desejado na árvore de equipamentos à esquerda, obter os dados sobre o equipamento e modificar os mesmos. Os campos disponíveis são idênticos aos campos da criação de equipamentos.

### 6.3.3 Reiniciação do Mecanismo de *Trapd*

Clicando sobre este campo é possível reiniciar o processo de *trapd* do sistema. Este processo é responsável por receber alarmes através de *Traps* de SNMP e redireccioná-los para os *emails* dos respectivos utilizadores configurados e para a base de dados.

### 6.3.4 Criação de um Grupo

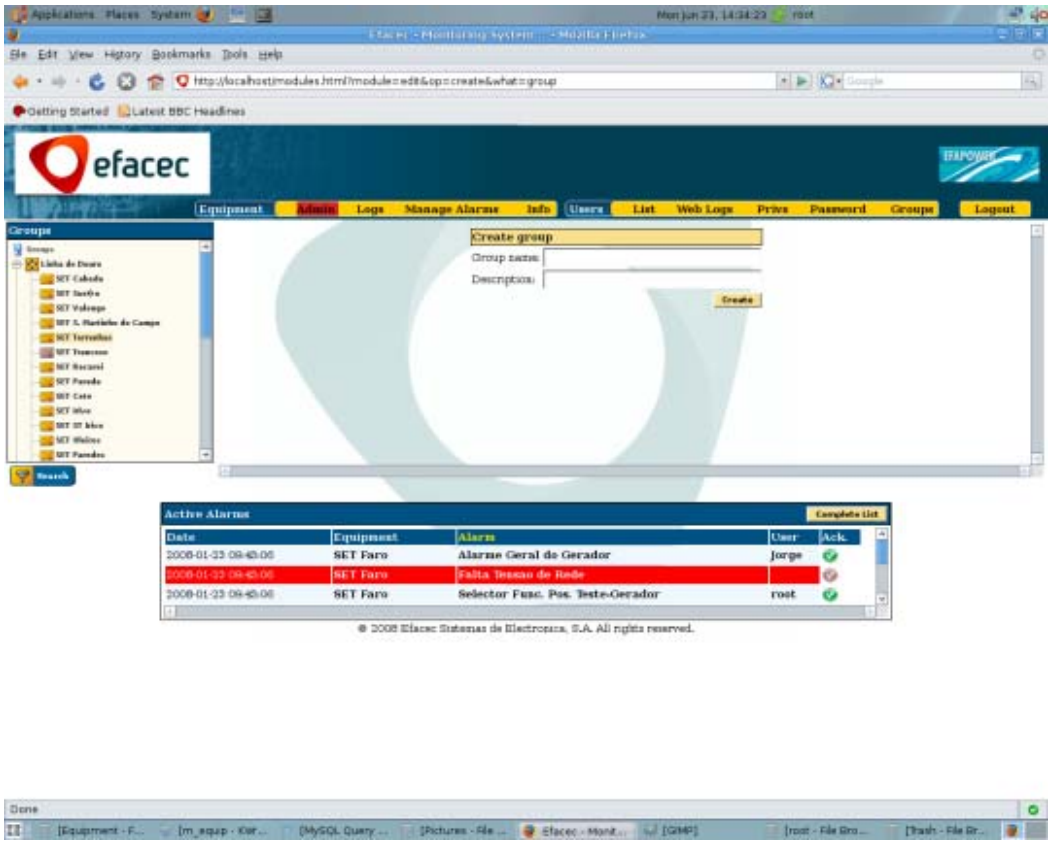


Figura 83 - Criação de um Grupo

Neste menu é possível criar um grupo de equipamentos. Podemos dar um nome ao grupo e ainda atribuir uma breve descrição do mesmo.

### 6.3.5 Modificação de um Grupo

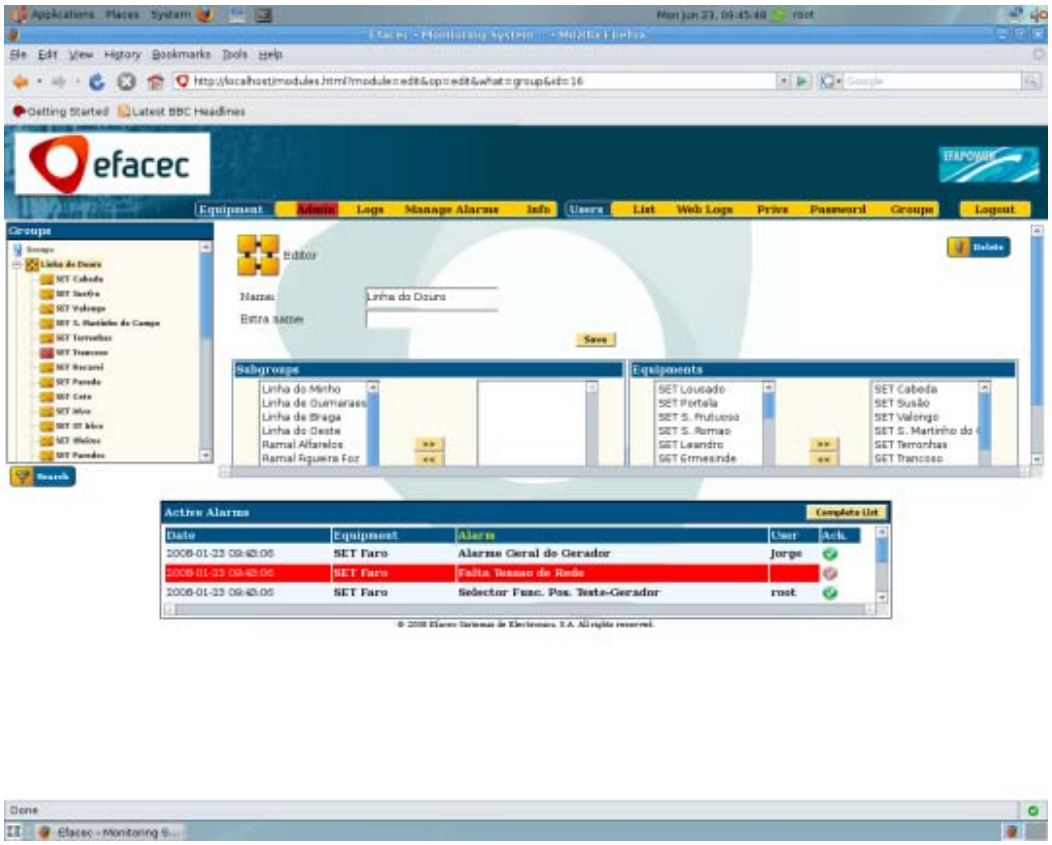


Figura 84 - Modificação dos dados de grupos

Clicando sobre um grupo de equipamentos na árvore de equipamentos à esquerda, podemos editar o grupo.

Podemos modificar o nome do grupo (*Name*) ou a descrição (*Extra name*). Existe um botão do lado direito do *frame* que permite apagar o grupo (*Delete*). O botão sob a árvore de equipamentos permite fazer uma pesquisa por equipamento desde que o utilizador conheça o nome do equipamento ou a sua localização, o IP ou até mesmo a *TagID* do equipamento que procura.

Neste mesmo menu é possível seleccionar quais os equipamentos disponíveis na base de dados que poderão fazer parte do grupo e, do mesmo modo, remover equipamentos do grupo.

## 6.4 Histórico de Alarmes

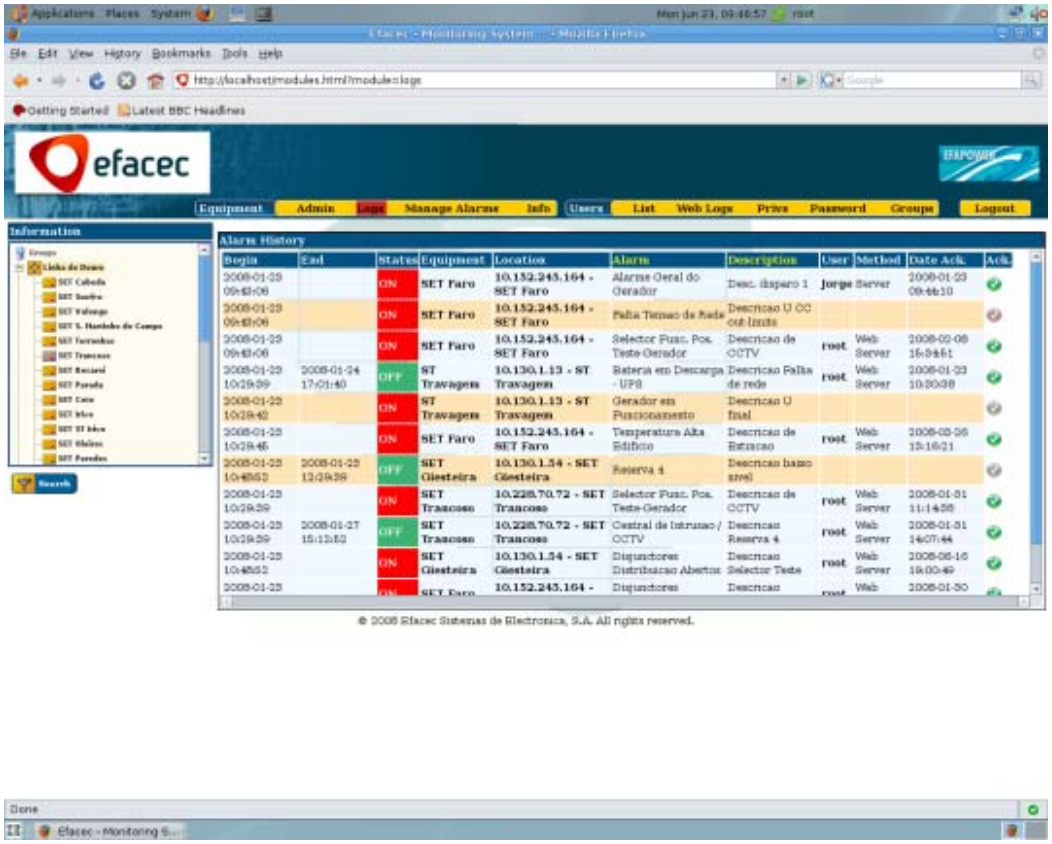


Figura 85 - Histórico de Alarmes

O menu histórico de alarmes apresenta a informação sobre o total de alarmes registados no sistema.

Regista a data de início do alarme (*Begin*), data de fim (*End*) quando deixa de estar activo, estado (*Status*), equipamento (*Equipment*), localização (*Location*), nome do alarme (*Alarm*), descrição do alarme (*Description*), utilizador que aceitou o alarme (*User*), método utilizado (*Method*) e data de aceitação (*Date Ack.*). A última coluna é constituída por botões para a aceitação dos alarmes por parte dos técnicos.

Tal como na tabela de alarmes activos, é possível reorganizar a mesma por cada um dos campos que a constitui. Clicando sobre um equipamento, da árvore de equipamentos temos acesso ao histórico de alarmes desse equipamento disponível na base de dados da aplicação *Web*.

## 6.5 Gestão de Alarmes

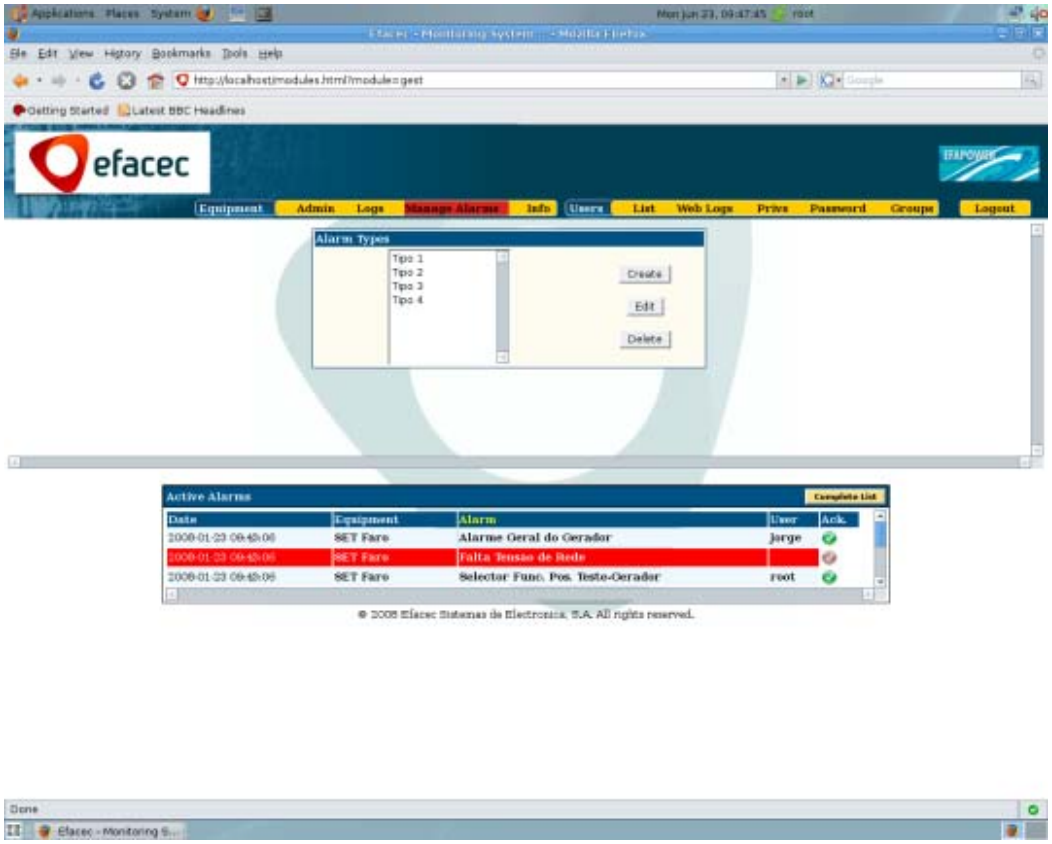


Figura 86 - Menu de Gestão de Alarmes

O menu de Gestão de Alarmes (*Manage Alarms*) permite definir diferentes configurações para cada tipo específico de alarme. Com estas configurações de alarme é possível determinar níveis de prioridade, níveis de alerta, *etc.* Este menu apresenta três opções para estas configurações:

- Criar (*Create*);
- Editar (*Edit*);
- Apagar (*Delete*);

### 6.5.1 Criação de uma Configuração de Alarme

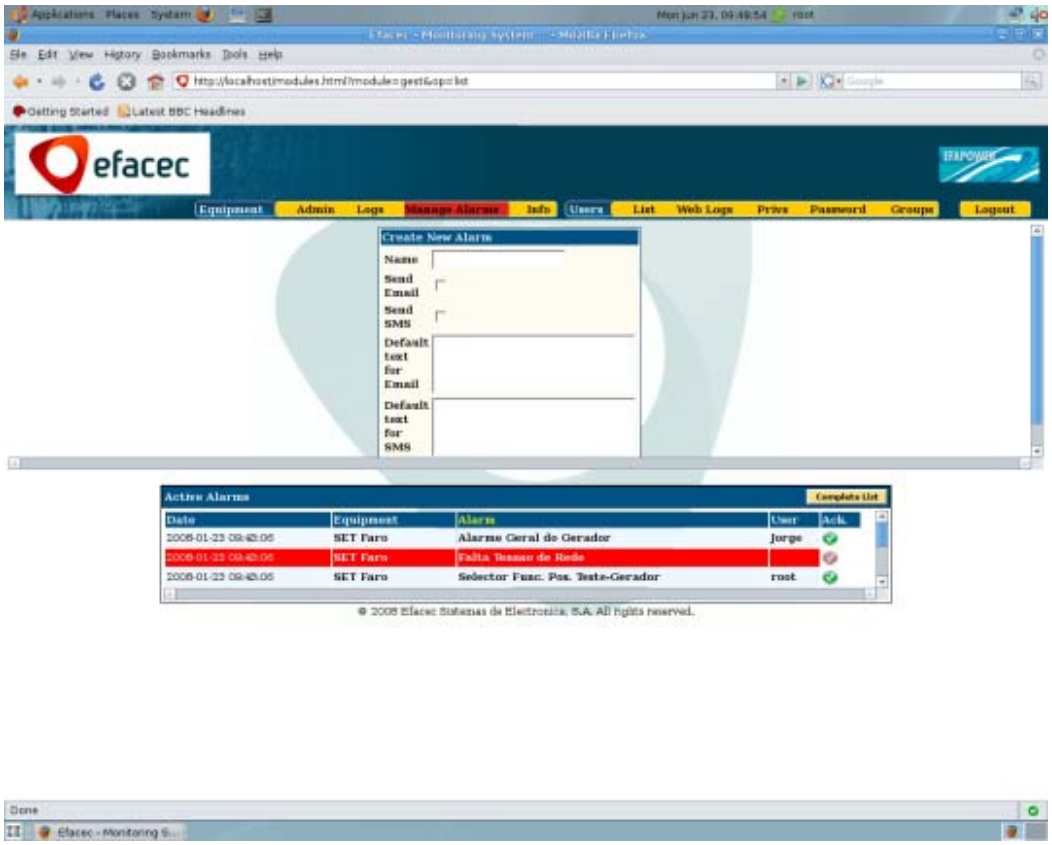


Figura 87 - Criar configuração de alarme

Neste menu, para além das *standard* de alarmes criadas originalmente, é possível criar um novo tipo de configuração de alarme.

Podemos definir o nome do equipamento (*Name*), activar as *flags* para envio de *Email* e envio de SMS (*Send Email* e *Send SMS,* respectivamente), introduzir um texto para ser enviado no *email* (*Default text for Email*) e para ser enviado na mensagem escrita (*Default text for SMS*).

### 6.5.2 Edição de uma Configuração de Alarme

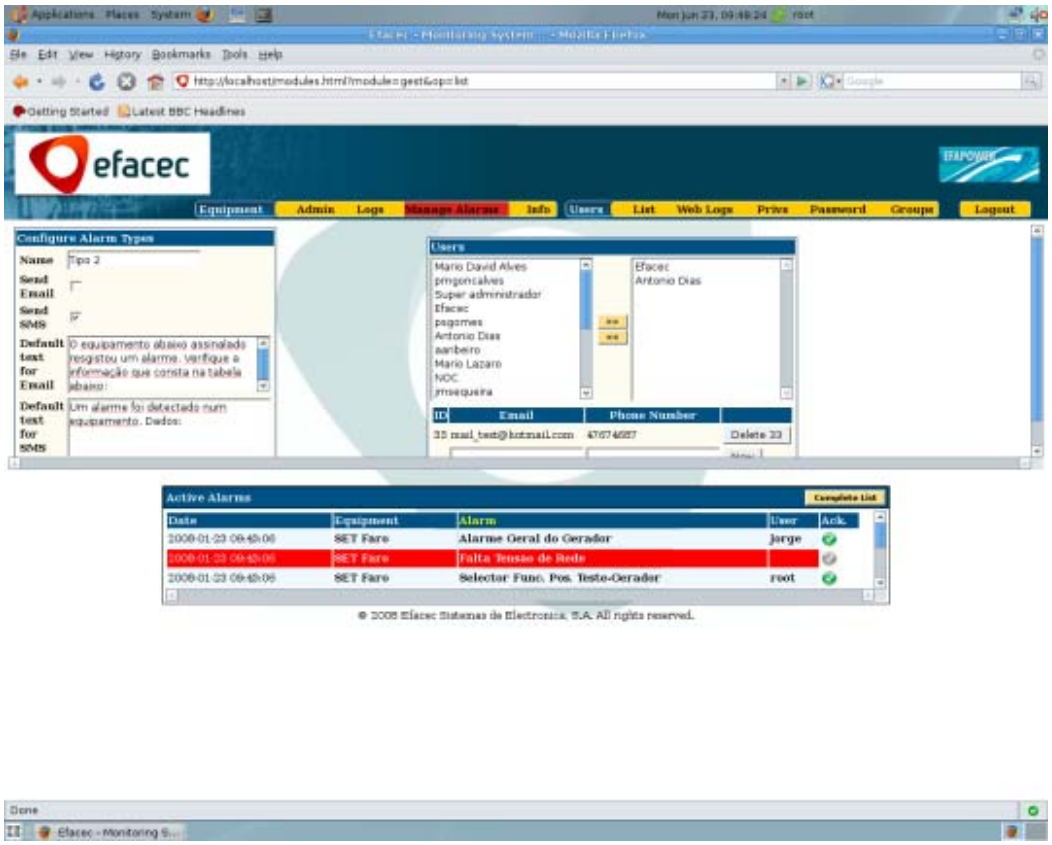


Figura 88 - Edição de Alarmes

Depois de criada a nova configuração de alarme, clicando sobre uma das configurações existente ou em Editar (*Edit*), temos acesso a todos os campos de configuração do alarme.

Além dos campos visíveis anteriormente, temos agora acesso a uma tabela na qual podemos associar utilizadores existentes na base de dados à configuração de alarme.

Está ainda prevista a possibilidade de serem introduzidos endereços de *email* e/ou números de telefone extra-utilizadores. É uma opção útil para introduzir dados adicionais para utilizadores que tenham mais que um endereço de *email* ou telemóvel ou para enviar alarmes para fora do circulo de utilizadores abrangidos pelo sistema.

## 6.6 Informação sobre Equipamentos

Este menu permite aceder directamente a um determinado equipamento, *i.e.,* para dele obter, em tempo real, todas as informações disponíveis.

Esta página apresenta um sinóptico central, uma tabela de alarmes activos do equipamento, um menu de *pop-ups* com informação útil sobre o sistema e uma tabela com os rectificadores ligados ao sistema.

### 6.6.1 Ligação por Modem

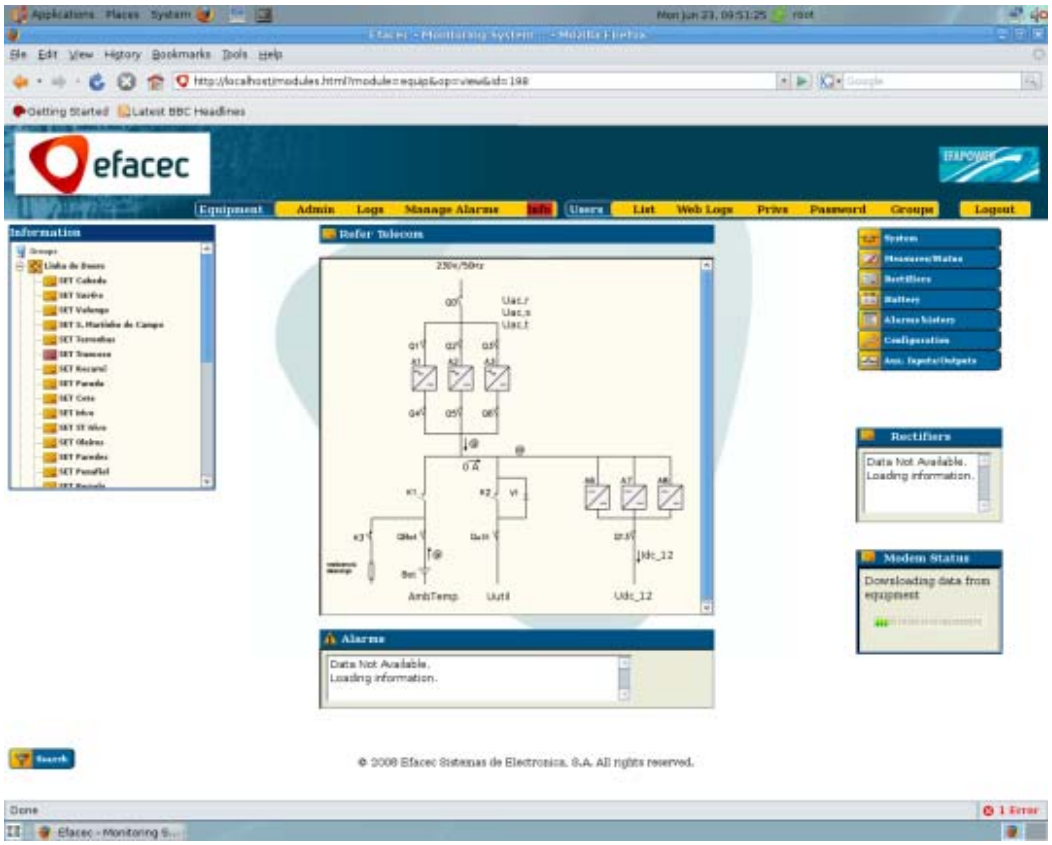


Figura 89 - Página de Informação de Equipamento (ligação por Modem)

No caso da ligação via modem, existe uma caixa informativa sobre o estado do modem. Nesta figura a informação do equipamento ainda se encontra a ser carregada para o sistema, pelo que está visível uma barra de carregamento de informação.

Devido às limitações de largura de faixa (*baudrate*) na leitura via interface série, os dados demoram cerca de 4 min até ficarem completamente disponíveis para consulta. A partir deste primeiro carregamento as actualizações são mais rápidas.

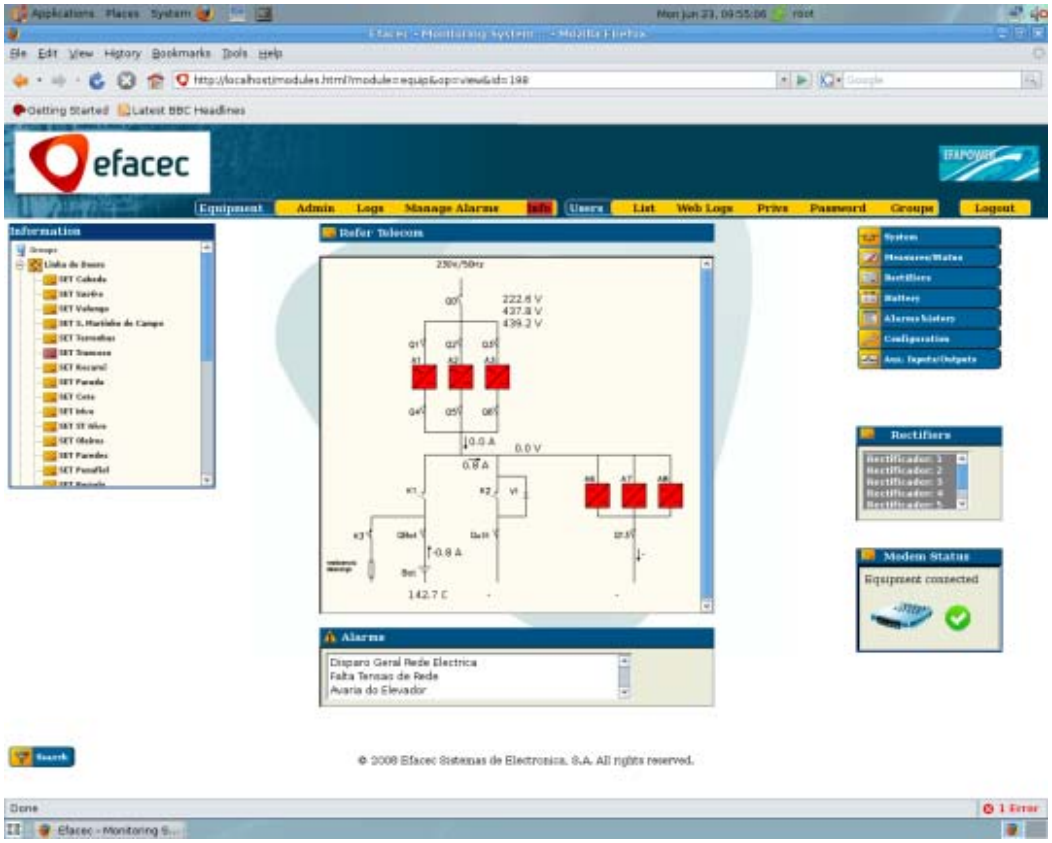


Figura 90 - Informação do equipamento após o carregamento de dados (Modem)

A tabela com o estado da ligação do modem mostra o estado actual da ligação, permitindo ao utilizador ter algum *feedback* sobre o que se está a passar a baixo nível.

É ainda possível desactivar a ligação através dos comandos incluídos nesta tabela.

### 6.6.2 Ligação por Rede

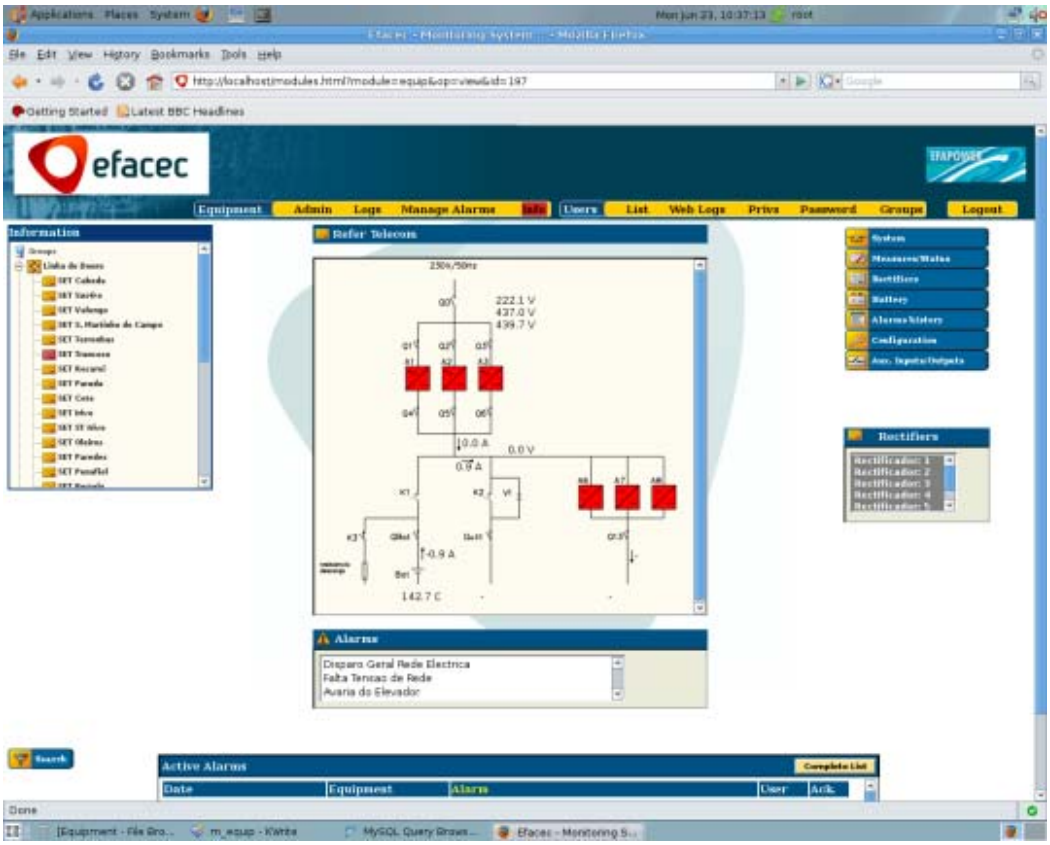


Figura 91 - Informação sobre equipamento (ligação com IP)

Ao contrário da ligação por modem, a ligação por rede (equipamento com IP atribuído) não apresenta o quadro com o estado da ligação. O menu de janelas apresenta a seguinte informação (para CIB):

- Sistema (*System*);
- Medidas/Estados (*Measures/States*);
- Rectificadores (*Rectifiers*);
- Bateria (*Battery*);
- Histórico de Alarmes (*Alarms History*);
- Configuração (Configuration);

- Entradas e Saídas auxiliares (*Aux. Inputs/Outputs*);

### 6.6.3 Janela de Sistema

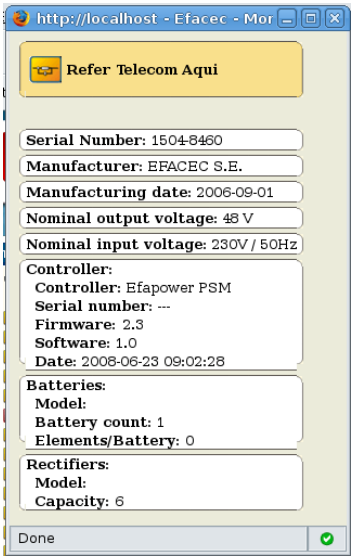


Figura 92 – Janela de Informação do Sistema

A janela de Sistema (*System*) apresenta informação relativa ao sistema do controlador (PSM). Entre os dados disponíveis estão o número de série do equipamento (*Serial Number*), o nome do fabricante (*Manufacturer*), a data de fabrico (*Manufacturing date*), a tensão nominal de saída (*Nominal output voltage*), a tensão nominal de entrada (*Nominal input voltage*), informações sobre o controlador, sobre as baterias e sobre os rectificadores presentes no CIB.

### 6.6.4 Janela de Medidas e Estados

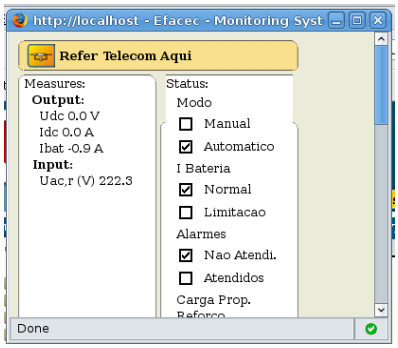


Figura 93 – Janela de informação sobre Medidas e Estados

Esta janela apresenta informação relativa a medidas disponíveis no PSM e aos seus respectivos estados.

### 6.6.5 Janela de Rectificadores

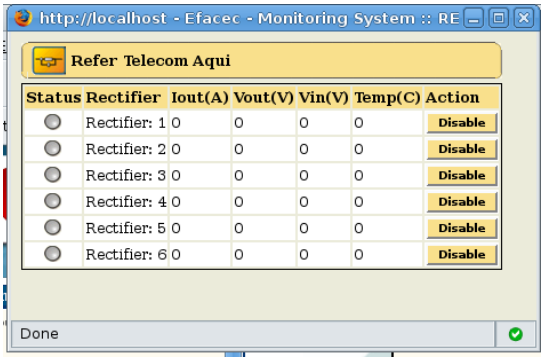


Figura 94 – Janela com informação sobre Rectificadores

Esta janela apresenta informação relativa ao estado dos rectificadores presentes no CIB. Permite ainda obter medidas de corrente de saída [Iout (A)], tensão de saída [Vout (V)], tensão de entrada [Vin (V)] e temperatura [Temp (ºC)].

Uma das opções disponíveis é a opção de desactivar os rectificadores.

### 6.6.6 Janela de Histórico de Alarmes


Figura 95 – Janela com histórico de alarmes do equipamento

Este janela apresenta o histórico de alarmes presente na memória do controlador do CIB.

### 6.6.7 Janela de Bateria

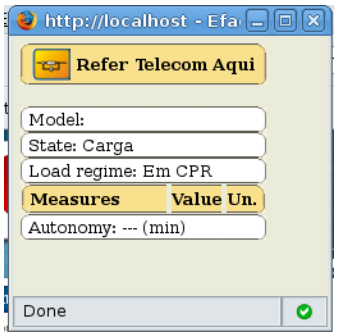


Figura 96 – Janela com informação sobre as Baterias

Esta janela apresenta informações acerta das baterias presentes no CIB, tais como o modelo (*model*), o estado (*state*), regime de carga (*load regime*) e até mesmo valores sobre a sua autonomia.

### 6.6.8 Janela de Configuração

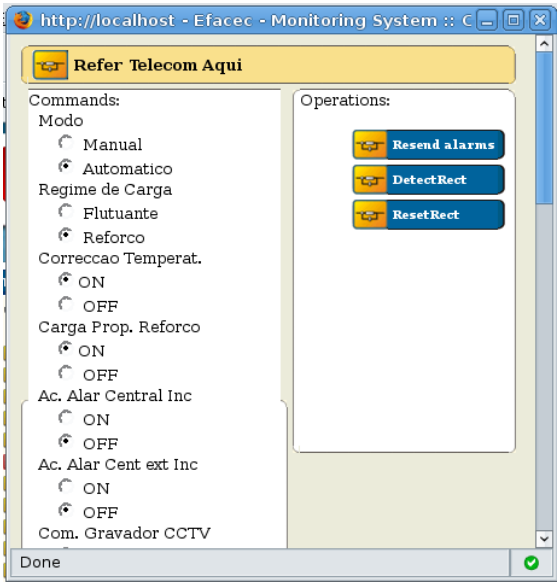


Figura 97 – Janela com comandos disponibilizados pelo PSM do equipamento

Esta janela apresenta um conjunto de comandos que se podem executar no controlador do CIB, permitindo actuar à distância sobre o mesmo. O conjunto de comandos depende das configurações de cada PSM.

### 6.6.9 Janela de Entradas e Saídas Auxiliares

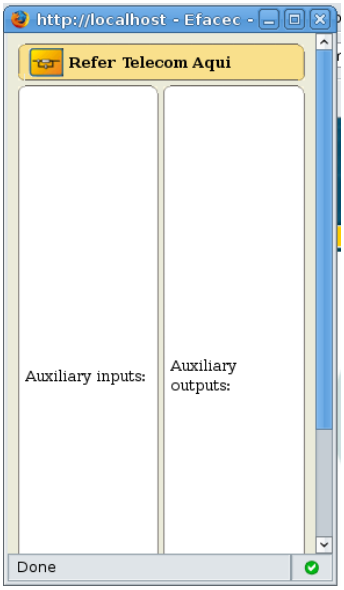


Figura 98 – Janela com informação sobre entradas e saídas auxiliares

Esta janela apresenta informação acerca da configuração das entradas e saídas auxiliares do CIB.

## 6.7 Listagem de Utilizadores

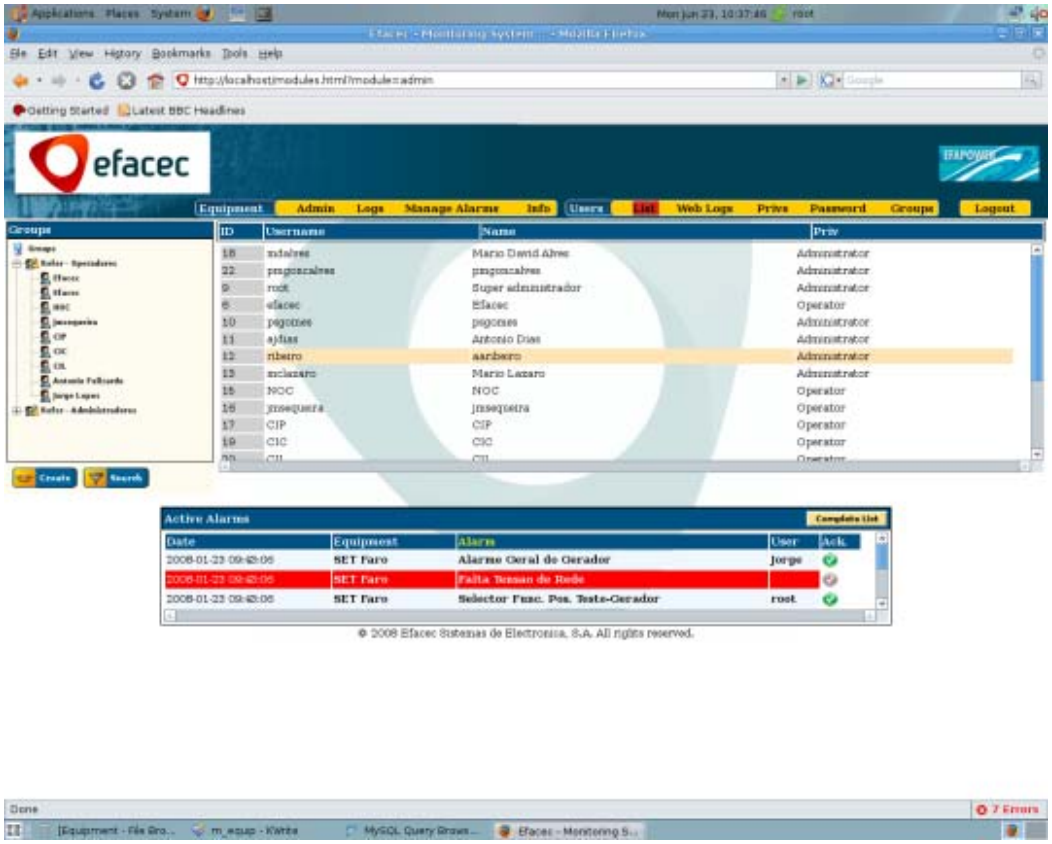


Figura 99 - Menu de listagem de utilizadores

No menu Listagem de Utilizadores (*List)* é apresentada a lista de todos os utilizadores registados no sistema.

A tabela é apresentada com a identificação única de cada um (ID proveniente da base de dados), o *Username*, o nome completo (*Name*) e o respectivo nível de acesso (*Priv*).

Do lado esquerdo aparece uma árvore idêntica à árvore dos equipamentos, mas com utilizadores, divididos em grupos.

Clicando sobre um dos campos da tabela ou sobre um utilizador da árvore de utilizadores, temos acesso aos dados desse utilizador. A figura abaixo exemplifica essa informação. Entre a informação disponibilizada temos o ID, o *username*, o nome completo (*Name*), dois campos para a senha (*Password*), *email*, número de telefone

(*Phone*), empresa (*Company*), identificação (*Identification*), posição (*Job*), tipo de acesso (*Type*), informações (*Information*) e linguagem (*Language*).

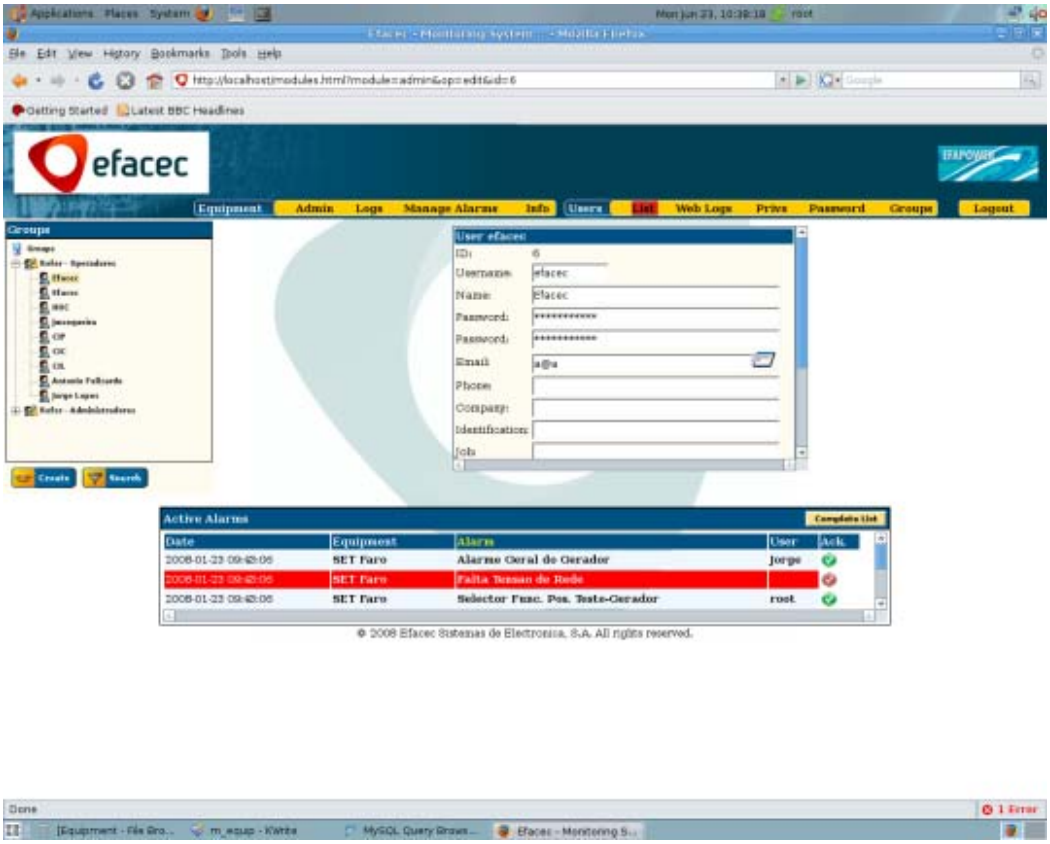


Figura 100 - Edição de utilizador

Debaixo da árvore de utilizadores estão dois botões. Um dos botões é de Procura (*Search*), que serve para pesquisar por utilizadores desde que o utilizador saiba qual o *username* nome ou tipo de utilizador que deseja pesquisar. O outro botão é um botão para adicionar (*Create*) um novo utilizador ao sistema, necessitando de se preencher os campos existentes.

## 6.8 Grupo de Utilizadores

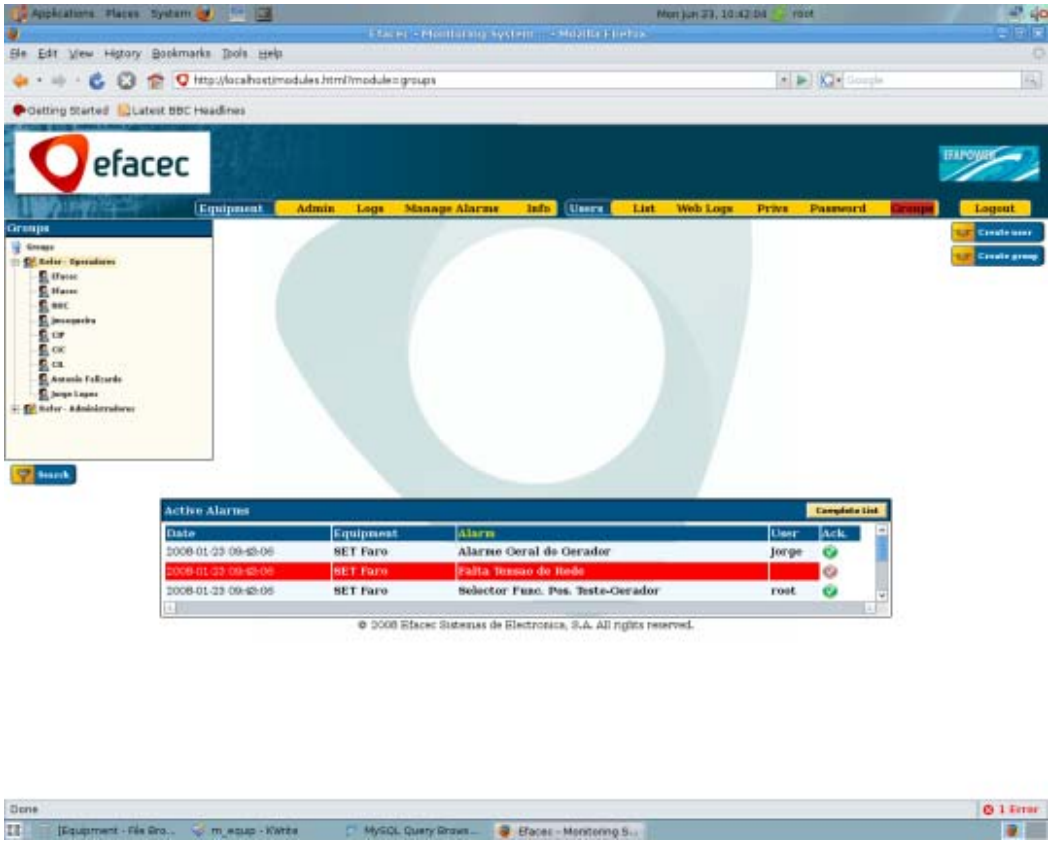


Figura 101 - Menu de Grupos de Utilizadores

Clicando sobre o menu grupo temos acesso a um menu que nos apresenta dois botões:

- Criar utilizador (*Create user*);
- Criar grupo (*Create group*).

### 6.8.1 Criação de um Grupo de Utilizadores

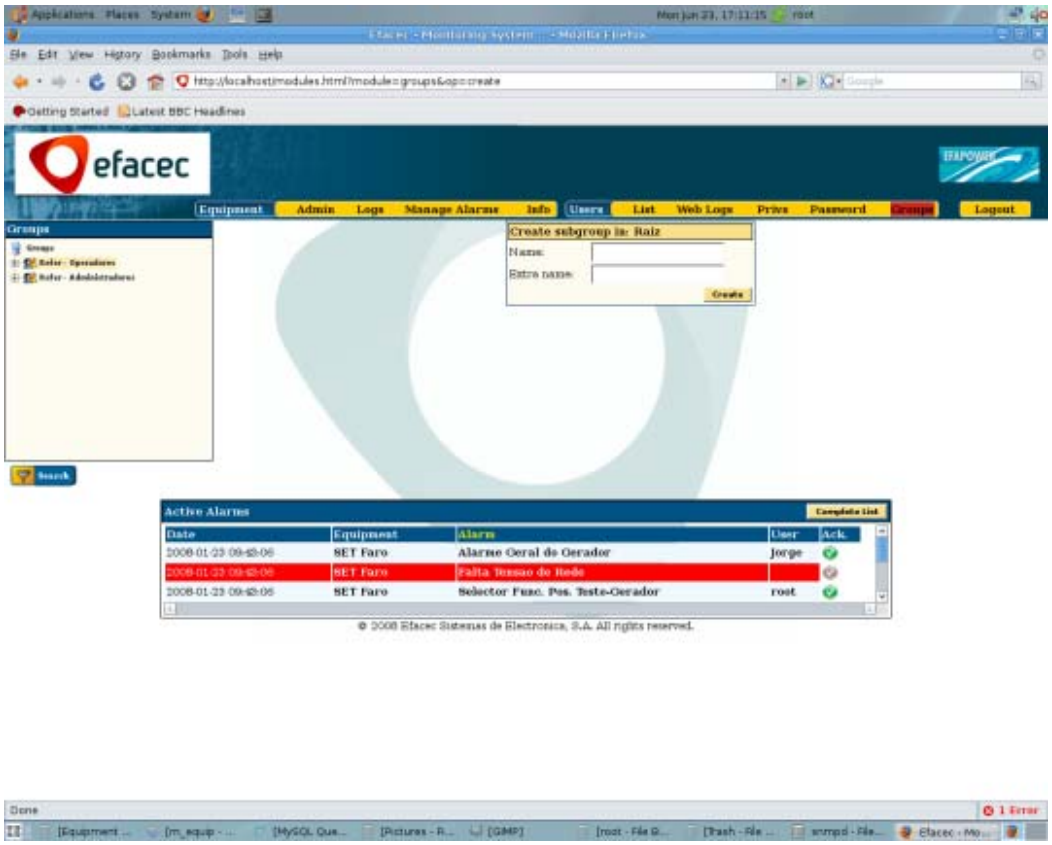


Figura 102 - Criação de um grupo de utilizadores

Clicando sobre Criar grupo (*Create group*), temos acesso a uma página onde nos é pedido o nome (*Name*) e uma descrição do grupo (*Extra Name*).

Apresenta um grafismo e lógica de funcionamento idêntico à criação de grupos para equipamentos.

### 6.8.2 Edição de um Grupo de Utilizadores

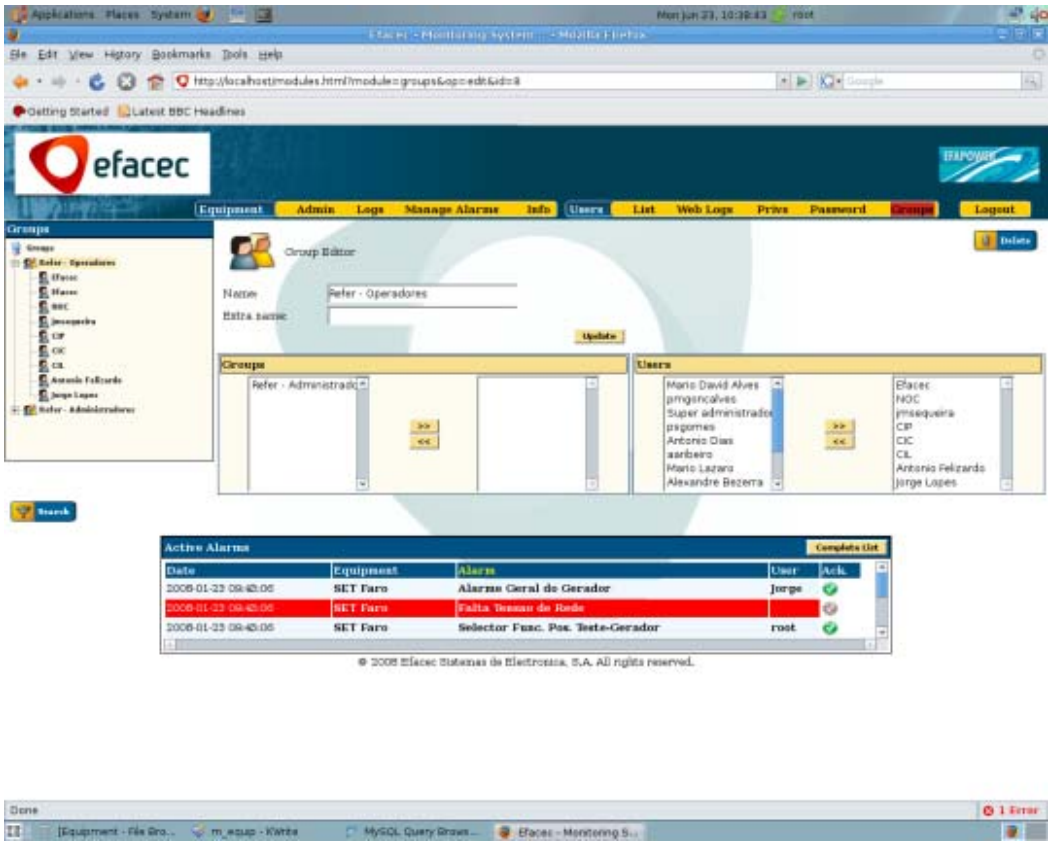


Figura 103 - Edição de grupo de utilizadores

No menu de edição de utilizadores temos acesso ao nome do grupo (*Name*), à descrição (*Extra Name*) e podemos seleccionar que utilizadores fazem parte deste grupo, adicionando-os ou removendo-os.

Apresenta um grafismo e lógica de funcionamento idêntico à edição de grupos para equipamentos.

## 6.9 Histórico de Acessos

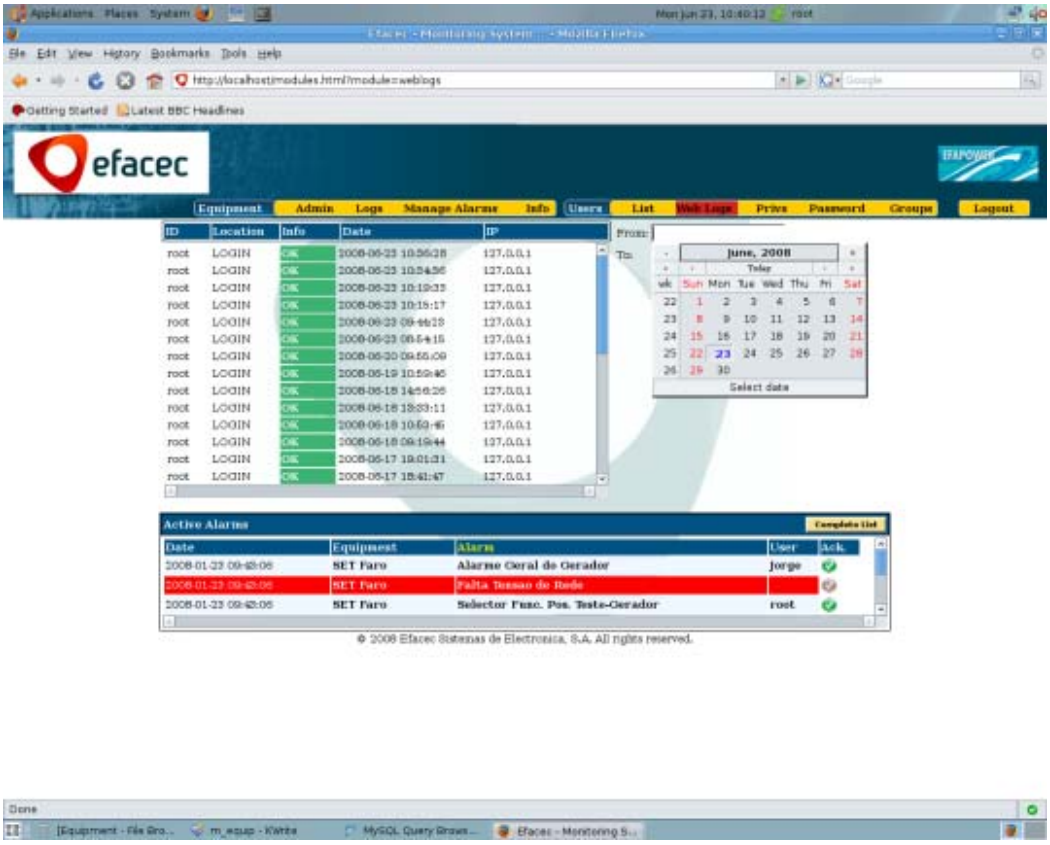


Figura 104 - Menu de controlo de acessos

No menu de histórico de acessos temos informação sobre quem acedeu à aplicação *Web*.

Esta informação é disponibilizada através de uma tabela dividida em identificação do utilizador (ID), localização (*Location*) (LOGIN/LOGOUT), informação acerca do acesso (*Info*) (OK/*ERROR*), data de acesso (*Date*) e IP, permitindo ainda detectar tentativas de acesso indevidas.

Podemos designar uma data de início e fim para circunscrever a tabela gerada ao período de um dia ou a um conjunto de dias específicos. A selecção das datas é efectuada através de um calendário em *JavaScript.*

## 6.10 Níveis de Acesso

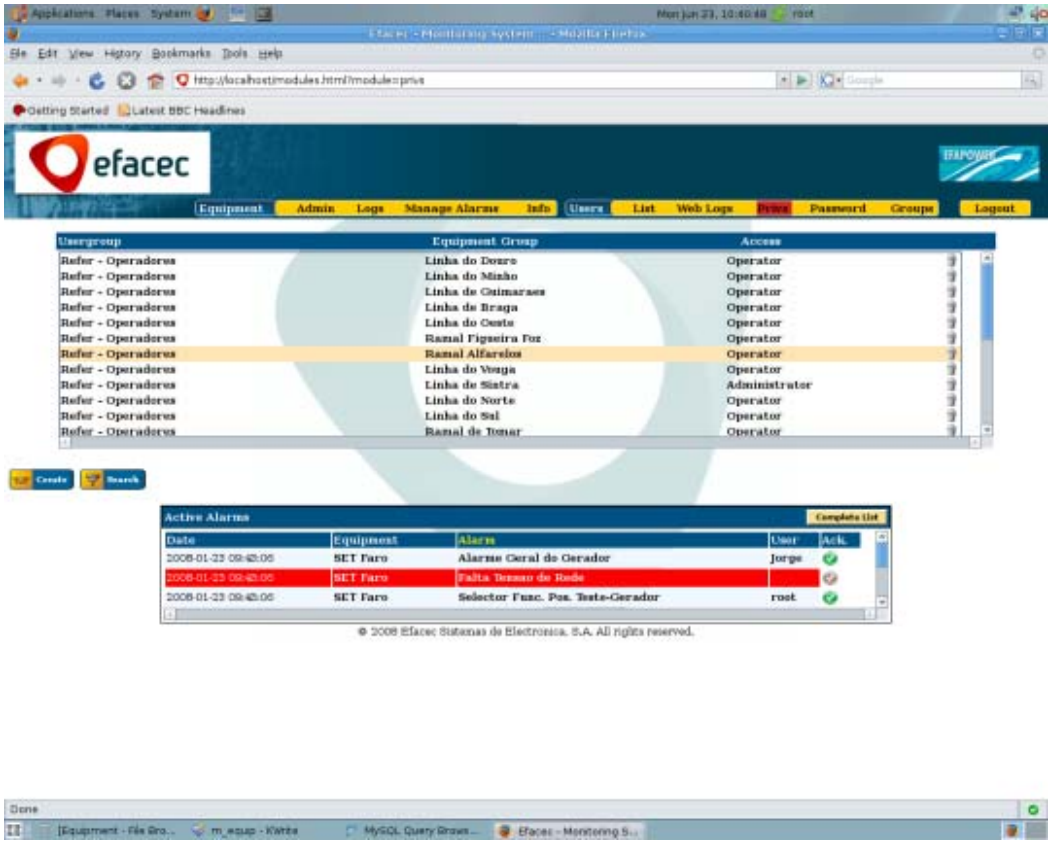


Figura 105 - Menu de edição de níveis de acesso

No menu de níveis de acesso é possível ver todos os níveis de acesso atribuídos a cada utilizador e as associações entre grupos de utilizadores e grupos de equipamentos.

Clicando sobre a coluna Acesso (*Access*) podemos modificar o nível de acesso atribuído.

Clicando no ícone do caixote do lixo apagamos a associação e nível de acesso existente.

## 6.11 Alteração da Senha

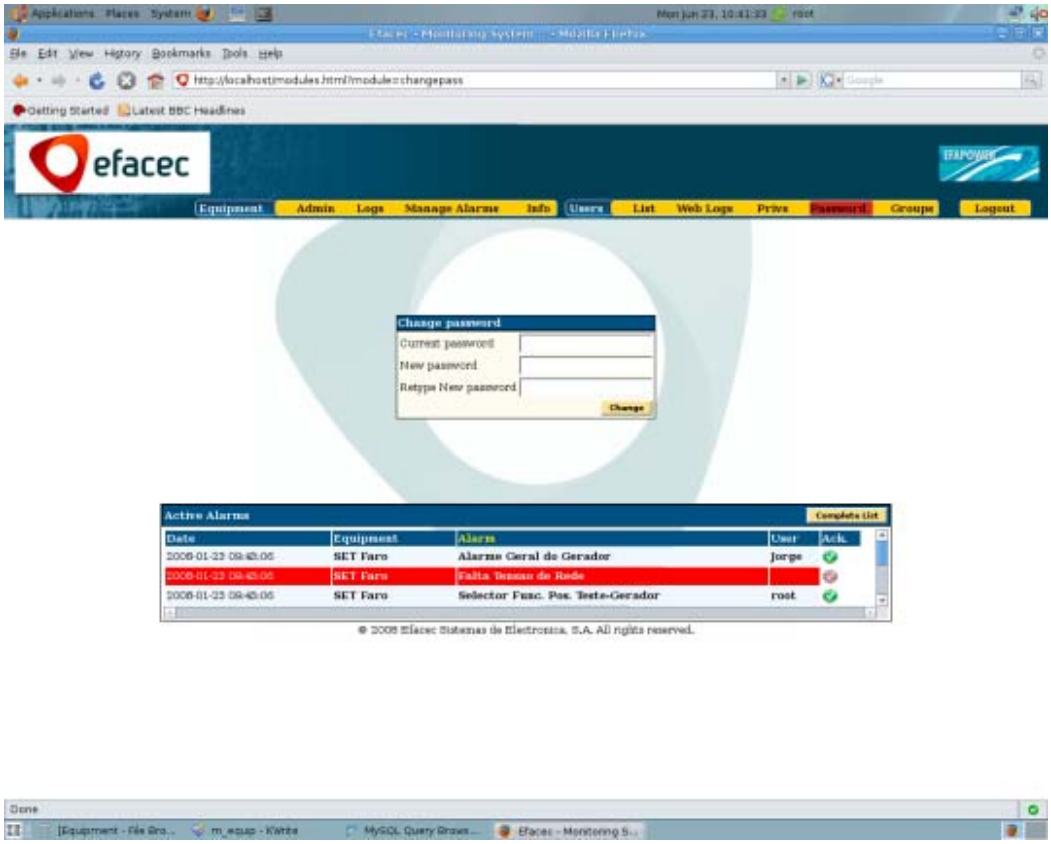


Figura 106 - Modificação da senha

No menu Senha (*Password*) podemos modificar a senha do utilizador corrente. Outra forma de fazer este passo seria editar o campo de senha no menu de edição do utilizador.

É necessário introduzir a senha actual (*Current password*), introduzir uma nova senha (*New password*) e reescrever a senha (*Retype New password*) por questões de segurança.

# 7 Conclusões

A aplicação desenvolvida apresenta várias funcionalidades que tornam possível o controlo sobre os equipamentos quer ao nível da sua configuração e desactivação de componentes em falha, quer no que diz respeito à monitorização dos mesmos.

A utilização de tecnologias recentes na aplicação *Web* permitiu melhorar a interacção com o utilizador, tornando a experiência de navegação entre as várias opções intuitiva. O refrescamento de dados de forma imperceptível ao utilizador permitiu aproximar o aspecto da aplicação *Web* a um *software* específico de monitorização e controlo de equipamentos, com a vantagem óbvia de centralizar toda a informação numa única máquina e base de dados.

Outra vantagem de se optar por uma aplicação *Web* para efectuar este tipo de função prende-se com o conceito de acessibilidade aos dados e equipamentos. Passa a ser possível a qualquer utilizador aceder ao sistema a partir de qualquer plataforma ligada à rede e com qualquer navegador. Não há necessidade de se centralizar o acesso num posto de controlo, como acontece em muitos centros de monitorização e controlo de equipamentos.

As múltiplas opções disponíveis para comunicar com os equipamentos vão de encontro às necessidades das empresas actuais. Embora o conceito de ligação em rede dos vários equipamentos seja largamente aceite, por questões de logística não é aplicado a todos os sistemas. Foi assim necessário implementar um sistema específico para comunicar com os equipamentos através de modems analógicos ligados por porta série. A interligação harmoniosa dos vários sistemas num mesmo conjunto é um dos grandes pontos fortes alcançados.

A gestão de alarmes permitiu uma resposta mais eficiente do sistema aos alarmes recebidos dos equipamentos. Permite uma resposta personalizada a cada tipo de alarme, possibilita alertar os técnicos de manutenção de forma directa e imediata e ainda registar um histórico de início e fim de alarme, utilizador que atendeu o alarme, data, *etc*.

Dada a formação académica, a adopção de uma arquitectura do tipo Mason e utilização da linguagem Perl surgiram como as duas principais dificuldades no desenvolvimento deste projecto. Foi necessária uma aprendizagem acelerada para ir de encontro às necessidades específicas do projecto. A integração de tecnologias AJAX e de sinóptico acabaram por ser elementos mais acessíveis dado o desenvolvimento efectuado anteriormente no projecto Efapower SNMP Webserver.

As principais limitações do sistema prendem-se com as funcionalidades ainda não desenvolvidas. O Efapower Webserver é um sistema em constante desenvolvimento que, obrigatoriamente, deverá crescer e tornar-se uma das mais completos soluções deste tipo no mercado. As comunicações por GSM para envio de alarmes, ligação à rede por Wi-Fi, são exemplos de módulos que poderão vir a ser desenvolvidos.

## 7.1 Instalação/Experiências

O Efapower Webserver é distribuído dentro de uma pasta *chroot*, bastando descompactar o mesmo para a raiz do sistema de ficheiro de um sistema operativo Linux através do comando:

```
tar -xvzf EFAPOWER_Webserver_v****.tar.gz
```

Depois de descompactar, basta aceder ao seu conteúdo e executar o *script start.sh* que automaticamente inicia todos os serviços:

```
cd /serviços/chroot/
./start.sh
```

Para interromper o funcionamento do servidor *Web*, basta digitar na linha de comandos:

```
./stop.sh
```

## 7.2 Avaliação do Desempenho da Solução Apresentada

Medir o desempenho de uma ferramenta de monitorização e controlo é sempre um processo complexo. Como a avaliar? Sobre que aspectos? Comparativamente a que outra ferramenta? Para facilitar este processo, fez-se uma avaliação qualitativa das

principais características do Efapower Webserver e uma avaliação quantitativa através de uma simulação de utilização.

Pretende-se com esta abordagem evidenciar os ganhos potenciais e reais que uma empresa poderá obter da utilização desta solução na monitorização e controlo dos CIB, além dos ganhos que este desenvolvimento trás para a própria EFACEC.

### 7.2.1 Vantagens do Sistema de Gestão Integrado

Uma das grandes vantagens que este sistema apresenta é a gestão de alarmes. Esta gestão permite uma diferenciação sobre o tipo de alarme recebido.

Através da consulta à base de dados, é possível determinar qual o grau de prioridade do alarme, se está configurado para enviar *email* ou SMS, a quem deve ser enviado um alarme por SMS ou *email*, *etc.* Com estas opções é possível enviar um *email* ou mensagem para um telemóvel com um texto próprio e informação sobre qual o alarme e equipamento em que ocorreu para vários utilizadores do sistema.

No caso hipotético de termos equipas de manutenção e assistência dispersas geograficamente, o alarme poderia ser enviado para os elementos da equipa mais próxima do equipamento com falha. Desta forma poderiam responder a este alarme um conjunto de técnico pré-determinado da base de dados.

A possibilidade de configurar individualmente os alarmes, atribuindo-lhes diferentes níveis de prioridade e diferentes acções, permite um controlo muito mais rigoroso e diferenciado sobre os mesmos. Desta forma, evita sobrecarregar o sistema com alarmes desnecessários e filtra os mais importantes para os agentes certos.

A ferramenta de reconhecimento (*acknowledge*) permite a qualquer pessoa que aceda ao sistema e veja o histórico, saber quem atendeu ou está a atender ao alarme, quando o fez, *etc.* Desta forma evita-se atender a um alarme já atribuído. Com este sistema evitam-se deslocações desnecessárias e permite-se ainda manter *online* o registo das assistências aos equipamentos.

### 7.2.2 Vantagens do Sistema de Acesso a Equipamentos

O acesso a equipamentos através de linha telefónica aumentou também o mercado sobre o qual este produto pode ser explorado. Para equipamentos colocados em localizações remotas ou em sistemas que conjuguem ligações por modem com ligações por Ethernet, este servidor apresenta-se como uma solução óbvia, suportando as mesmas funcionalidades que no caso de ligação de rede, mas com as limitações impostas pelo meio.

A integração de sistemas que estão contactáveis por SNMP e por uma infra-estrutura com suporte para linha analógica traz vantagens a este sistema face aos anteriores. É possível monitorizar e controlar, virtualmente, todos os equipamentos deste tipo (CIB e UPS) de uma determinada empresa, tanto os mais antigos como os mais recentes. Esta abordagem possibilita ainda a integração de equipamentos de outras empresas e de outro tipo.

### 7.2.3 Vantagens do Controlo Remoto sobre Equipamentos

Tal como o próprio conceito indica, este sistema não só é capaz de monitorizar, mas também consegue interagir remotamente com os sistemas.

É possível ao utilizador aceder às opções de configuração de gestão do controlador do equipamento e intervir sobre o mesmo. Pode, assim, ser possível resolver alguns problemas relacionados com o equipamento à distância, evitando uma deslocação ao local. Podem ser desligados componentes defeituosos (se disso não resultar prejuízo para o equipamento, performance, *etc.*) para mais tarde ser feita uma manutenção ao equipamento. Noutros casos, componentes podem ser reiniciados remotamente, tais como rectificadores. Este tipo de operação, geralmente simples, evita deslocações desnecessárias, permitindo uma redução de custos com melhoria na disponibilidade de serviço.

### 7.2.4 Problemas Associados a Ferramentas Anteriores

Uma normal implementação deste tipo de sistema passava por concentrar toda a informação do sistema num controlo central do tipo SCADA.

Este controlo central reunia todas as informações relativas a alarmes, estados dos equipamentos, *etc.* Um dos principais problemas que resultava deste sistema era que todos os alarmes eram enviados sem diferenciação para o sistema central. No sistema central seria recepcionado um alarme que proviria de um determinado sistema, sem uma indicação clara sobre o tipo específico de problema que tinha afectado a máquina. A indicação normal passava pela utilização de contactos secos que normalmente definiam quatro níveis de prioridade de alarmes. Dependendo destes níveis, o alarme seria ignorado ou seria alertado um técnico para fazer a assistência ao equipamento.

Este alarme seria enviado para um *front-end* do sistema SCADA, necessitando de um técnico na sala de controlo que revisse todos os alarmes recebidos e actuasse em conformidade com o que o sistema sugeria. De facto, seria este técnico a alertar os técnicos da área afecta ao alarme da necessidade de deslocação ao local da avaria.

Deste processo resultaria um excesso de alarmes que necessitaria de uma filtragem sistemática, de forma a definir como proceder à assistência, quem enviar ou não para o campo e munido de que peças sobresselentes. O problema associado ao excesso de alarmes passaria, desde logo, pelo tempo que demoraria a atender a cada alarme, a definir se seria um alarme importante ou ignorável, quem seria enviado para o local, *etc.*

Outro problema associado ao sistema anterior passaria pela possibilidade de apenas definir um endereço de correio electrónico associado a cada equipamento. Poderia ser definido um *email* de um técnico de assistência mas com várias condicionantes:

- A mensagem de alarme descriminava o tipo de alarme, apenas referindo o equipamento;

- Não havia sistema implementado de confirmação de alarme, pelo que o sistema não saberia se o *email* foi ou não recebido;

- O alerta de alarme (*email*) apenas poderia ser recebido pelo técnico de assistência quando este estivesse num local com acesso à Internet.

### 7.2.5 Aplicação Típica

Este sistema apresenta as suas maiores vantagens na gestão da assistência aos equipamentos. É um sistema que permite filtrar, automatizar e simplificar o processo de assistência a um equipamento, sendo integrável com outros sistemas. Desde logo, o facto de o sistema ser acessível através de um qualquer terminal ligado à Internet, com um qualquer *browser*, independentemente do sistema operativo, permite-lhe ser utilizado por um grande número de pessoas e acedido de qualquer sítio. Esta vantagem torna-o excelente para ser utilizado por equipas de manutenção de campo, permitindo-lhes utilizar esta ferramenta como referência no seu trabalho.

Para evidenciar algumas dessas vantagens, será feita uma demonstração do processo que é desencadeado quando não está disponível este tipo de sistema e quais as diferenças resultantes (com a ressalva que estes processos variam de cliente para cliente, dependendo da sua estratégia operacional). Este caso baseia-se em empresas reais, clientes deste tipo de sistemas da EFACEC, discriminando o nome, função e número de aparelhos adquiridos. O estudo efectuado deverá levar a uma redução do número de efectivos necessários para efectuar as operações de monitorização e assistência.

NOTA: Estes dados foram estipulados a partir de conversas com elementos do Departamento de Desenvolvimento da unidade de negócio.

Tipificando a empresa *Y* com cerca de 200 equipamentos distribuídos geograficamente de Norte a Sul do país, com distâncias que variam entre 5 km a 80 km entre si. Cada um destes equipamentos (CIB e UPS) está ligado a um equipamento importante (tais como subestações e centrais de telecomunicações), sendo a sua alimentação vital para o bom funcionamento do sistema. Cada vez mais há da parte das empresas uma maior exigência na elevada disponibilidade de serviço. Se por cada hora que um determinado equipamento estiver desligado a empresa tiver um prejuízo, convém que a assistência seja breve e eficaz.

Para que a área geográfica ficasse coberta por uma rede de assistência, a empresa A define dois centros de assistência com dois técnicos cada. Utilizando o sistema antigo (de controlo centralizado num sistema do tipo SCADA, o Scatex), seria recebido um alarme através de um contacto seco de um equipamento. Este alarme seria redireccionado para o *front-end* (HMI) de interacção com o técnico de monitorização e gestão do sistema. Este, dependendo do nível do alarme associado, contactaria um técnico de assistência para assistir o equipamento ou ignoraria o alarme. O contacto com o técnico poderia passar por um *email* ou telefonema. Deste alarme resultaria uma quantidade muito reduzida de informação sobre o equipamento e a única maneira de aceder ao sistema seria deslocando-se ao local.

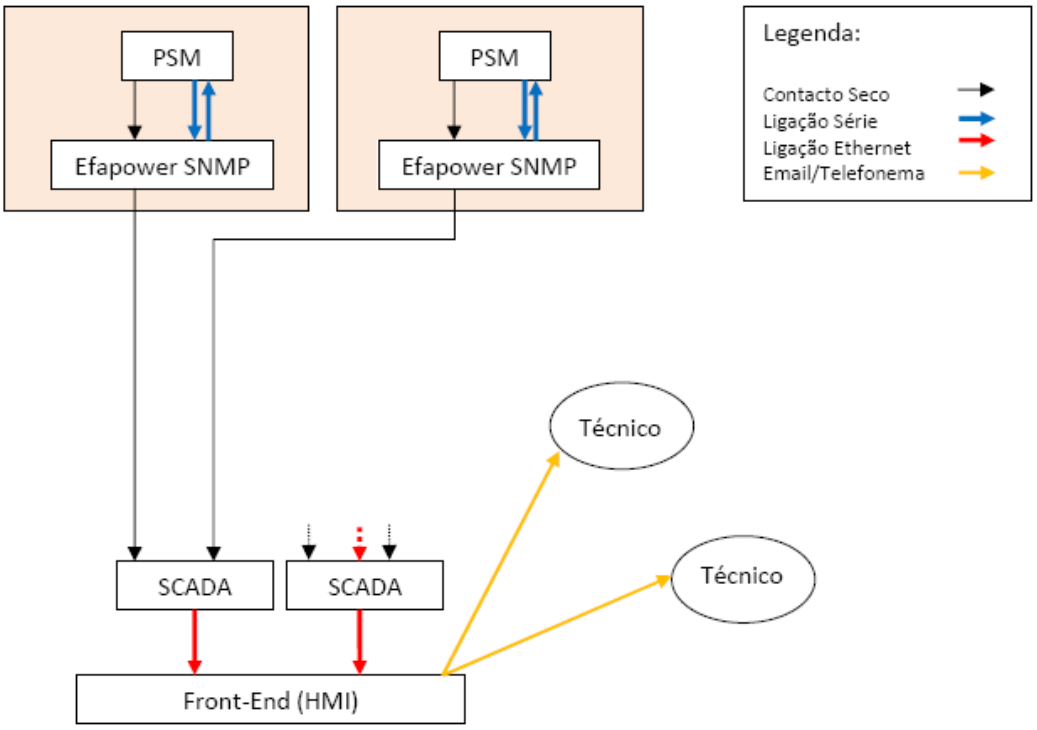


Figura 107 – Ligação por contactos secos sem Efapower Webserver

#### 7.2.5.1 Monitorização

Este sistema não permite aos técnicos aceder directamente ao equipamento, muitas vezes por haver uma restrição de acessos por questões de segurança. Ora, sem aceder ao sistema, a manutenção preventiva fica seriamente comprometida, permitindo apenas uma assistência a falhas. Para efectuar uma manutenção preventiva aos diversos equipamentos, seria necessário aos vários técnicos

deslocarem-se com uma determinada periodicidade aos locais onde se encontravam colocados os equipamentos. Seguindo o exemplo do nosso caso teórico, para 200 equipamentos, distanciados entre si numa média de 10 km, obteríamos um valor da distância percorrida pelo técnico de 2000 km:

10 km x 200 equipamentos = 2000 km

Se o técnico se deslocar num carro comercial a gasóleo, com um consumo médio por quilómetro de 5 l aos 100 km, teremos, após aritmética simples, 100 litros de gasóleo consumido. A um preço de cerca de € 1,40/l (valor médio em vigor em Julho de 2008), teríamos um custo de € 140,00 para realizar a deslocação completa.

Se a este custo associarmos o tempo despendido para o acesso, manutenção e/ou reparação de equipamentos, teremos cerca de 30 min por cada equipamento (cerca de 10 min de viagem e uma média de 20 min para restantes operações). O tempo estipulado para acesso ao equipamento incluí aceder ao equipamento, ligar o equipamento a um portátil, carregar dados para o portátil, analisar dados e efectuar uma verificação visual final. Este tempo é variável, dependendo das operações de manutenção que sejam necessárias efectuar. Assim, para percorrer o total de equipamentos desta empresa *Y*, seriam necessários cerca de:

30 min x 200 equipamentos = 6000 min

6000 min / 60 min = 100 h

Resumindo, para que um único técnico fizesse a monitorização a todos os equipamentos no local, seriam necessárias cerca de 100 h e custos de € 140 associados apenas a deslocação. Seria possível à empresa definir a periodicidade desta ronda de manutenção pelos equipamentos de forma a manter os equipamentos em bom funcionamento, diminuindo a probabilidade de falhas.

Incluindo o EFACEC Webserver no sistema, teremos um sistema paralelo que permite outro nível de acesso e gestão. Desde logo o EFACEC Webserver conecta aos equipamentos através da Internet (seja ao módulo SNMP como na figura, ou por um modem analógico) e consegue remotamente obter muito mais informação dos

equipamentos. Além disso, as comunicações são bidireccionais, permitindo não só receber dados dos equipamentos, mas também enviar dados para os equipamentos.

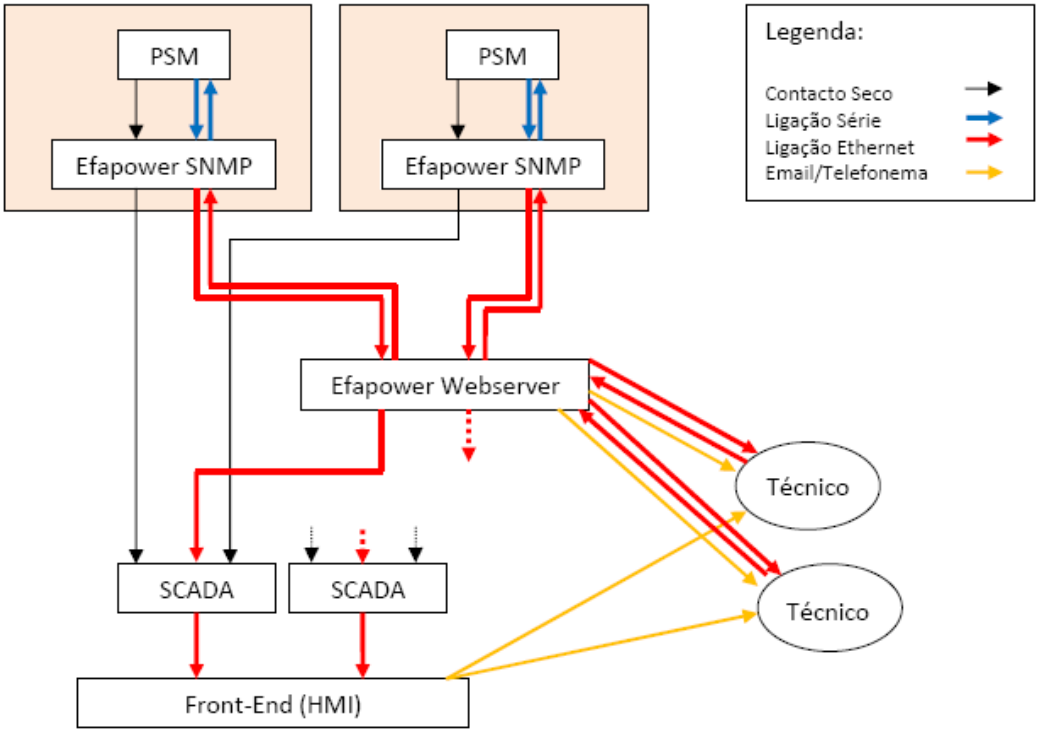


Figura 108 – Ligação por contactos secos com Efapower Webserver

Assim, em termos de monitorização dos equipamentos, será possível a um só técnico abrir uma sessão no Webserver e ligar a cada um dos equipamentos a que esteja autorizado a aceder, obtendo as mesmas informações do sistema que obteria junto do equipamento. Além disso, tem ainda a possibilidade de efectuar alterações à configuração do equipamento e controlador.

Por outras palavras, tirando a inspecção visual do equipamento, a completa monitorização do equipamento pode ser efectuada remotamente através do Efapower Webserver. Com a utilização deste recurso, será possível reduzir a periodicidade da ronda de manutenção, limitando esta a uma mera inspecção visual da condição dos equipamentos.

Neste novo cenário, para cada equipamento, há que aceder aos diversos menus de configuração e verificar todos os parâmetros. Esta operação poderá demorar cerca de 5 min para uma ligação com largura de faixa larga (tempo médio

para verificar as principais informações do PSM) e cerca de 10 min a 15 min para uma ligação com largura de faixa estreita (ligação por modem que inclui ligar o modem, obter dados e desligar o modem). Para verificar o conjunto dos 200 equipamentos teremos:

Para ligação de faixa larga:

5 min x 200 equipamentos = 1000 min

1000 min / 60 min = 16,7 h

Para ligação de faixa estreita:

15 min x 200 equipamentos = 3000 min

3000 min / 60 min = 50 h

Como em termos de ligações estes sistemas integram equipamentos com ligações de rede e sistemas com ligações por modem, é natural que o valor real de tempo despendido para a completa monitorização do sistema se encontre entre os dois valores acima atingidos. Como tal, comparando com o tempo despendido numa monitorização dos equipamentos com e sem Efapower Webserver, teremos uma diminuição entre 83,3 % (para equipamentos ligados por faixa larga) e 50 % (para equipamentos ligados por faixa estreita).

Se a esta diminuição de tempo adicionarmos a não necessidade de nos deslocarmos ao local para a recolha de dados, temos que acrescer a poupança que decorre em termos de gastos com os combustíveis e logística da deslocação. Dado que a inspecção periódica aos equipamentos é sempre recomendável, este sistema não elimina por completo este tipo de deslocações, mas reduz drasticamente a sua periodicidade.

Em termos demonstrativos, se a empresa *Y* tiver uma periodicidade de monitorização dos equipamentos de uma ronda em cada duas semanas, terá, ao fim de um ano, um total de 26 rondas de monitorização. Sem o Efapower Webserver para apoio à monitorização, ao fim de um ano teremos um acumular de 2600 h

associadas a rondas de monitorização e um custo de € 3640 em despesas de combustível.

Tempo:

100 h * 26 rondas = 2600 h

Despesas de combustível:

€ 140 * 26 rondas = € 3640

Utilizando o Efapower Webserver para apoio à monitorização teremos que assumir que a cada 4 rondas através do Webserver, uma será feita localmente para garantir a inspecção visual (este número é variável e dependerá da política da própria empresa). Assim teremos:

Com inspecção no local:

100 h * 7 rondas = 700 h

€ 140 * 7 rondas = € 980

Com inspecção remota:

Faixa Larga:

17 h * 19 rondas = 323 h

Faixa Estreita:

50 h * 19 rondas = 950 h

Tabela 6 – Custos e tempos associados à monitorização de equipamentos

| *Hipótese* | *Ligação* | *Tempo (h)* | *Custo (€)* |
|---|---|---|---|
| Sem Efapower Webserver | - | 2600 | 3640 |
| Com Efapower Webserver | Faixa Larga | 1023 | 980 |
| | Faixa Estreita | 1650 | 980 |

Analisando a tabela, podemos ver que, para o caso estipulado e sem prejuízo para o número de monitorizações a que cada equipamento está sujeito, há, no

melhor dos casos, um ganho de mais de 60 % em termos de tempo e uma redução de mais de 70 % no custo. Para o pior dos casos, teremos um ganho médio de mais de 35 % em termos de tempo e de 70 % em termos de custos.

Estes valores estão associados a apenas um custo operacional (custo do combustível) e ao tempo utilizado para as várias operações. Do ponto de vista empresarial, o custo real cifra-se no número de técnicos necessários e custo de técnico por dia.

Para que seja possível demonstrar que este sistema leva a uma redução do número de técnicos ou equipas de manutenção necessárias, vamos estipular que o preço de custo de um técnico de manutenção por dia é de € 250. Este valor englobará o salário, custos de deslocação, material, *etc.* Consideremos que a empresa *Y* deseja que a ronda de monitorização seja toda efectuada no espaço de um dia, sem turnos, ou seja 8 horas úteis.

Aplicando algumas regras de cálculo simples teremos:

Total de horas necessárias para ronda de monitorização / Tempo de execução por técnico = Números de técnicos necessários

Sabendo o tempo total que é necessário para efectuar a monitorização completa aos equipamentos da empresa (já determinado atrás) e sabendo que cada técnico, num turno, apenas trabalha oito horas úteis (8 h), dividimos um valor pelo outro e obtemos o número de turnos que um técnico precisaria de fazer para completar a tarefa. Se a cada turno associarmos um técnico, será possível efectuar a monitorização de todo o sistema no tempo desejado. Assim, para um sistema que não tenha o Efapower Webserver incorporado, teremos:

100 h / 8 h = 12,5 turnos

Concluindo o raciocínio, necessitaríamos de, no mínimo, 13 técnicos distribuídos por toda a área geográfica para conseguir monitorizar a totalidade dos equipamentos.

Para o mesmo caso, mas utilizando o Efapower Webserver como parte integrante no sistema, teríamos:

17 h / 8 h = 2,1 turnos Ligação por Faixa Larga

Resultando em 3 turnos, ou seja, 3 técnicos. No caso dos equipamentos ligados por modem seriam necessários 7 técnicos para efectuar a ronda de manutenção:

50 h / 8 h = 6,25 turnos Ligação por Faixa Estreita

Tabela 7 – Tabela de técnicos necessários para cada ronda de monitorização

| *Hipótese* | *Ligação* | *N.º de Técnicos* | *Custo de equipa (€)* |
|---|---|---|---|
| Sem Efapower Webserver | - | 13 | 3250 |
| Com Efapower Webserver | Faixa Larga | 3 | 750 |
| | Faixa Estreita | 7 | 1750 |

Na tabela acima calculou-se o custo total de uma ronda de monitorização dos equipamentos a partir do valor estipulado para o custo diário de um técnico (€ 250). Desta forma foi possível atingir um valor de custo para o total da operação neste caso específico. Estes valores de custo são variáveis (devido a custo de manutenção específicos, alteração dos custos por técnico, *etc.*) e servem como elementos meramente indicativos para a obtenção da relação entre valores.

Sem o Efapower Webserver, para garantir uma elevada disponibilidade de serviço e cumprir a estratégia operacional da empresa *Y*, são necessários 13 técnicos, com um custo associado de € 3250. Utilizando a ferramenta desenvolvida neste projecto, necessitaremos, no melhor dos casos, de 3 técnicos a um custo de € 750 ou, no pior dos casos, de 7 técnicos a um custo total de € 1750. Em termos percentuais, a empresa Y poderá reduzir o número de técnicos associados a esta operação em valores que poderão variar entre 77 % e 46 %, dependendo da estrutura do próprio sistema. Os custos teriam um redução proporcional, respeitando a lógica estipulada.

Em conclusão, o maior ganho pode se encontrar ao nível dos custos com o pessoal técnico necessário. Para uma empresa esse factor é essencial. Qualquer

corte ao nível de custos de operação que não traga prejuízo ao serviço, traz apenas vantagens. Outro factor, cada vez mais importante, é o tempo despendido em cada operação. Como há uma diminuição do tempo associado a esta operação, a empresa pode agregar menos efectivos a esta tarefa ou optar por aumentar o número de operações de monitorização, aumentando a disponibilidade do serviço sem que isso acarrete gastos adicionais.

#### 7.2.5.2 Assistência a Alarmes

No caso anterior analisaram-se os ganhos que esta solução traz para os clientes em termos de monitorização dos equipamentos. Neste capítulo a análise será feita sobre a questão da assistência a alarmes, se bem que de uma forma mais qualitativa que quantitativa, uma vez que estes eventos são aleatórios. Ao contrário do que acontecia com a monitorização, em que se implementavam rotinas, estas ocorrências são esporádicas e dependem de muitas variáveis.

Um sistema que não integre o Efapower Webserver terá, obrigatoriamente, que ser integrado num sistema de gestão do tipo SCADA. Este sistema permite monitorizar os alarmes provenientes dos equipamentos através de contactos secos e determinar a sua origem e tipo de alarme. Estão definidos, por norma, quatro contactos secos, variando entre si o nível de prioridade. Em alguns sistemas podem ser definidos muitos mais contactos secos, discriminando cada um dos alarmes existentes no equipamento. Neste último caso será possível ao operador do SCADA fornecer dados acerca do tipo específico de alarme que recebeu ao técnico que contacta, permitindo que este possa agir em conformidade. Caso contrário, no sistema mais geral, apenas pode informar o técnico de qual o tipo de alarme recebido (*e.g.* grave ou muito grave) e de que equipamento o recebeu.

Com estes dados em mão resta ao técnico dirigir-se até ao local para determinar qual a falha e, caso seja necessário, repará-la. Neste caso, duas situações podem ocorrer:

Situação A: É necessária a substituição de um determinado componente;

Situação B: É apenas necessária uma alteração ao nível da configuração do controlador.

Na situação A poderá ocorrer que o técnico não vá munido da peça necessária para a substituição, necessitando de regressar para a ir buscar. Nesta operação perde-se tempo e acrescem os custos de deslocação. Não é concebível que um técnico traga consigo todos os componentes de um CIB, sendo expectável que traga apenas os componentes mais susceptíveis a falhas.

Utilizando o sistema de gestão de alarmes do Efapower Webserver, o sistema principal de gestão não fica invalidado, mas passa a ser apoiado. Por outras palavras, o técnico ainda pode ser informado pelo controlo central, mas é lhe fornecida informação extra relativa ao alarme. Além de receber um *email* ou *SMS* imediatamente após a recepção do alarme no Webserver, esse *email* ou *SMS* discrimina imediatamente o tipo de falha que o equipamento sofreu. Desta forma, é possível levar equipamento próprio para a reparação da falha, salvaguardando a situação A.

Se a falha for de um tipo que permita a sua resolução através de um acesso ao controlador do CIB ou UPS, o técnico pode, através do Efapower Webserver, aceder ao equipamento remotamente e efectuar as mesmas configurações que faria no local. Esta seria a resolução para a situação B. Além de permitir uma resolução muito mais rápida do problema, evita deslocações ao local desnecessárias. Há aqui um ganho tanto em termos de tempo como em termos de custos.

Outra variante do sistema de gestão de alarmes passa pela atribuição do alarme a um técnico. É possível aceitar o alarme e associar o nome do técnico responsável pelo atendimento. Este sistema garante que apenas um técnico é destacado para o local, evitando que mais que um técnico acorra à mesma falha no equipamento. Como é óbvio, este sistema permite evitar mais deslocações desnecessárias.

Este sistema permite, assim, libertar o operador do sistema SCADA da gestão da logística associada à assistência a falhas nos equipamentos e garante homogeneidade de atendimento a alarmes.

O facto do acesso ao Efapower Webserver ser possível a partir de qualquer terminal com acesso à Internet, torna-o passível de ser utilizado em toda a área geográfica abrangida pela empresa *Y*.

Em suma, utilizando esta ferramenta para gestão de alarmes, é possível ter uma intervenção mais rápida, mais eficaz e menos susceptível a sobreposições de atendimentos. Evitando deslocações desnecessárias, reduzem-se os custos. Aumenta-se a qualidade dos serviços de assistência ao permitir que os técnicos possam com base nos dados recebidos seleccionar o material e analisar o problema antes de chegarem ao local. Diminui-se também o tempo despendido no total das assistências se diminuirmos viagens desnecessárias e implementarmos o uso de configurações remotas através do Efapower Webserver.

Não sendo possível quantificar os ganhos em termos de custos e de tempo, dada a natureza aleatória das falhas, é contudo visível que há grandes vantagens na utilização deste sistema por parte do cliente.

#### 7.2.5.3 Ganho para a EFACEC

O ganho para a empresa EFACEC, uma vez que não comercializa esta ferramenta separada dos seus produtos CIB e UPS, passa pelo aumento do grau de satisfação dos clientes e pelo aumento das funcionalidades que passa a disponibilizar nos seus produtos. Além deste produto dar vantagem competitiva à EFACEC sobre outros produtos semelhantes de concorrentes e servir como factor decisório na fase de escolha, este produto pode oferecer funcionalidades aos clientes que contribuam para um aumento dos lucros (por intermédio de uma optimização de recursos). Este aumento de lucros e de satisfação do cliente deverá, em princípio, garantir a fidelidade e dependência de um cliente a um produto EFACEC, abrindo novas portas a outras aquisições.

Não é, portanto, um produto que ofereça um ganho directo para a empresa mas sim um produto que oferece um ganho competitivo, de imagem e de técnica.

## 7.3 Trabalho Futuro

Esta secção identifica alguns aspectos da aplicação que podem vir a ser melhoradas.

A evolução gráfica de um mapa com a referência geográfica da localização dos equipamentos deverá ser implementado para dar uma referência visual muito mais prática na gestão dos alarmes. Poderá ajudar a definir qual ou quais dos técnicos deverão fazer a assistência a equipamentos com problemas.

A comunicação por GSM deverá ser implementada. Há grandes vantagens em localizações remotas e que não têm ligação a redes telefónicas ou redes LAN. Desde que a zona seja coberta pelo sistema GSM, o equipamento estaria contactável.

A evolução da base de dados para acomodar equipamentos UPS, além dos CIB, está prevista e parcialmente implementada. Por questões de ordem temporal não foi possível implementar por completo este aspectos.

Um módulo de gestão inteligente de equipamentos também poderá ser implementado. Este módulo permitiria avançar com sugestões de soluções para alarmes ao utilizador e, em alguns casos, actuar automaticamente sobre os equipamentos.

No caso de o sistema ter acesso à localização geográfica dos técnicos, poderia ser possível enviar missões de assistência automaticamente para o técnico mais próximo, evitando custos de deslocação desnecessários.

Outra evolução interessante seria a adaptação da configuração da página *Web* de monitorização para PDA. Desta forma, os técnicos poderiam recorrer apenas a um PDA para terem acesso à informação do sistema.

Em anexo segue-se o trabalho de conceptualização que foi efectuado após um estudo de mercado e de tecnologias existentes e antes de o projecto ter sido

iniciado. Esse artigo tem toda a informação necessária para a compreensão do conceito e funcionalidades que foram previstas. Entre essas funcionalidades encontram-se as que já foram implementadas e as que ainda não foram.

## 7.4 Apreciação Final

O Efapower Webserver completa o conjunto de três principais ferramentas de monitorização e controlo de CIB disponibilizados pela EFACEC Sistemas de Electrónica, desenvolvida pelas unidade de Sistemas de Alimentação.

O Efacon é um *software* desenvolvido para ser executado num sistema operativo Windows da Microsoft. Tem a capacidade para se conectar a um ou vários equipamentos através de SNMP. O Efapower SNMP Webserver é um servidor de HTTP que disponibiliza as mesmas funcionalidades do menu de Informação de Equipamento do Efapower Webserver. Apenas oferece as funcionalidades relativas ao equipamento a que o módulo SNMP está associado. Fornece a capacidade de um CIB ser conectado a uma rede LAN.

A principal diferença deste produto sobre os restantes prende-se com o facto de poder controlar todo o conjunto de CIB ou UPS que uma empresa possua, permitindo um controlo e monitorização realmente distribuído por todo um conjunto de utilizadores do sistema. Permite ainda o acesso a uma base de dados comum e a um histórico de alarmes comum do sistema, funcionado um pouco como um controlo central.

Tirando proveito desta característica, o Efapower WebServer poderá evoluir até um ponto em que se torne uma referência nesta família de produtos, tornando-se muito mais versátil e capaz de um controlo inteligente, evoluindo do conceito de central de monitorização para o de aplicação distribuída com naturalidade. Nesse sentido, aproximar-se-ia do conceito dos sistemas SCADA, apesar de mais direccionado para a manutenção e assistência técnica dos equipamentos.

Ao introduzir o conceito de gestão diferenciada de alarmes e módulos de comunicação mais abrangentes, este sistema permite alertar técnicos que se

encontrem no campo através de SMS e permite a confirmação da recepção do alerta.

A confirmação de alarmes evita que dois ou mais técnicos respondam ao mesmo alarme e permite ainda saber, por simples consulta ao equipamento, a quem foi atribuída a intervenção no equipamento. Desta forma, o sistema permite algum nível de gestão automática das assistências.

Todas estas características reflectem-se numa redução dos custos operacionais para uma empresa que esteja envolvida na manutenção de sistemas de equipamentos de alimentação distribuídos, aumentando ainda a disponibilidade de serviço que esta pode oferecer, o que torna este produto muito atractivo neste tipo de mercado.

# 8 Bibliografia


- *BARBOSA, Ricardo - Projecto WINCON II - Interface Remota de Controlo e Aquisição/Visualização de Dados, EFACEC – Sistemas de Electrónica S.A., FEUP, 2007, JUN*

- *PETERSEN, Theo - Web Development with Apache and Perl. Manning, 2002. ISBN 1-930110-06-5*

- *MGE UPS Systems – Network Management Cards, http://www.mgeups.com/products/pdt120/software/multslot/html/SNMPweb.htm*

- *Generex Intelligent UPS Network, http://www.generex.de/e/products/additional/cs111/cs_120_p.shtml*

- *Eltek Valere, http://www.eltek.com/wip4/detail.epl?cat=9335*

- *Rectifiers Technologies, http://www.rtp.com.au/*

- *Unipower Telecom, http://www.unipowertelecom.com/Telecom_Product_Line/telecom_product_line.html*

- *Tycon Electronics, http://www.tycoelectronics.com/*

- *Redes, http://www.redes.xl.pt*

- *Mason HQ, http://www.masonhq.com*

- *CPAN, http://www.cpan.org*

- *MySQL, http://www.mysql.com*

- *The Perl Directory, http://www.perl.org*

- *Basic Hayes AT Command, http://modemhelp.net/basicatcommand.shtml#M*

## 8.1 Índice de Referências

*[1] in "EFACEC Home Page" (http://www.efacec.pt )*

*[2] in "Efapower Home Page" ( http://www.Efapower.efacec.pt )*

*[3] in "SCADA – Automation Solutions Center" (http://scada.atspace.com/)*

*[4] in "SCADA – Wikipédia" (http://en.wikipedia.org/wiki/scada)*

*[5] in " Mini Power Supply Manager" (MiniPSM bilingue A1.pdf)*

*[6] in "Efapower SNMP" (Catálogo EFAPOWER SNMP.pdf)*

*[7] in "Galaxy Pulsar Plus" (Galaxy Pulsar Plus.pdf)*

*[8] in "*Galaxy Millenium™ Controller*" (Galaxy_Millenium.pdf)*

*[9] in "*PCM 500 Series*" (pcm500-revA-01-08-02.pdf)*

*[10] in "*DSC 1000 Series*" (dsc1000-ds.pdf)*

*[11] in "*DSC 1000 Series Manual*" (dsc1000-man.pdf)*

*[12] in "*GALAXY Gateway v3*" (Gateway.pdf)*

*[13] in "*Smartpack*" (smartpack.pdf)*

*[14] in "*WebCSU*" (WebCSU [W1760a].pdf)*

*[15] in "*Manual CS121*" (CS121.pdf)*

*[16] in "*Network Management Cards-User manual*" (Mge ups Network Management Cards User Manual.pdf)*

*[17] in "*Power Supply Manager*" (psm(sa18b9910b1)_pt-ing.pdf)*

*[18] in "*SENA Hello Device*"*
*(http://www.sena.com/products/device_servers/wireless/hd_lite/)*

*[19] in "*SENA Hello Device*"*
*(http://www.sena.com/products/device_servers/external/hd_super/)*

*[20] in "*MiniCSU-2 110V*" (Spec MiniCSU-2 5BW1656b5D.pdf)*

*[21] in "***WEP - Wikipédia***" (http://pt.wikipedia.org/wiki/WEP)*

*[22] in "***Implementar, optimizar e garantir a segurança Wi-Fi***"
(http://www.redes.xl.pt/99/400.shtml)*

*[23] in "LanPro 11/31T Uninterruptible Power Supply" (Application and Technical_GEAD1508CE_PDF.pdf)*

*[24] in "Sistema de Informação Remota via Internet (IRIS)"
(http://www.geindustrial.com.br/produtos/ups/iris_01.asp)*

*[25] in "Sistema de Informação Remota via Internet (IRIS)"
(http://www.geindustrial.com.br/produtos/ups/iris_02.asp)*

*[26] in "Dynamic UPS UNIBLOCK" (piller rotary ups 1006 – eng.pdf)*

*[27] in "Gama de UPS" (UPS-EFACEC.pdf)*

*[28] in "Wi-Fi – Segurança"
(http://www.dei.unicap.br/~almir/seminarios/2006.1/ns06/wifi/pg_wf_seguranca.html)*

*[29] in "Padrão Serial RS-232" (http://www2.eletronica.org/artigos/eletronica-digital/padrao-serial-rs-232)*

*[30] in "Simple Network Management Protocol"
(http://pt.wikipedia.org/wiki/Simple_Network_Management_Protocol)*

*[31] in "MODBUS" (http://pt.wikipedia.org/wiki/Modbus)*

*[32] in "PROFIBUS" (http://pt.wikipedia.org/wiki/Profibus)*

*[33] in "eWON" (http://ewon.be/)*

*[34] in "HP Open View" (http://en.wikipedia.org/wiki/OpenView)*

*[35] in "HP Network Node Manager"
(http://en.wikipedia.org/wiki/Network_Node_Manager)*

*[36] in "HP Network Node Manager Software System and Device Support Matrix
(http://support.openview.hp.com/selfsolve/document/KM309084/binary/releasenotes.html#DeploymentGuide)*

*[37] in "HP Network Node Manager Software" (hp_man_NNM800_Deployment_pdf.pdf)*

*[38] in "List of network management systems"
(http://en.wikipedia.org/wiki/List_of_Network_Management_Systems)*

*[39] in "IBM Tivoli Framework" (http://en.wikipedia.org/wiki/IBM_Tivoli_Framework)*

*[40] in "Tivoli Intelligent Orchestrator 5.1"*
*(http://publib.boulder.ibm.com/infocenter/tivihelp/v14r1/index.jsp?topic=/com.ibm.tivoli.tpm.ept.doc/agent/ccas_casovwagent.html)*

*[41] in "Siemens IT Solutions and Services"*
*(http://www.pse.siemens.at/apps/sis/en/pseInternet.nsf/CD_Index?OpenFrameset&Bookmark&/0/PKFE5BA4C7F83C707AC12569EE003A4A5A)*

*[42] in "Nagios Wikipédia" (http://en.wikipedia.org/wiki/Nagios)*

*[43] in "Nagios 3.x manual" (http://nagios.sourceforge.net/docs/nagios-3.pdf)*

*[45] in "Galaxy Manager" (http://power.tycoelectronics.com/Family.aspx?FID=5ac72702-3b27-4297-bbcb-061c5e62a278)*

*[46] in "Galaxy Manager Manual" (93104107-gateway_manual.pdf)*

*[47] in "SAFT WinSite" (http://www.harmerandsimmons.com/software/winsite.html)*

*[48] in "ENEC"*

*(http://products.emersonenergy.com/sales/products/displayproduct.asp?id=1188&PGroup=All)*

*[49] in "EXMG"*

*(http://products.emersonenergy.com/sales/products/displayproduct.asp?id=139&PGroup=All)*

*[50] in "EMAS"*

*(http://products.emersonenergy.com/sales/products/displayproduct.asp?id=83&PGroup=All)*

*[51] in "GeMSi" (http://www.gamatronic.com/home/page.aspx?id=208&lang=1)*

*[52] in "MGE UPS Supervision System"*

*(http://www.mgeups.com/products/pdt230/software/supervise.htm)*

*[53] in "HTML Wickipédia" (http://pt.wikipedia.org/wiki/HTML )*

*[54] in "JavaScript Wickipédia" (http://pt.wikipedia.org/wiki/JavaScript )*

*[55] in "AJAX Wickipédia" (http://en.wikipedia.org/wiki/Ajax_(programming)*

*[56] in "Perl Wikipédia" (http://pt.wikipedia.org/wiki/Perl)*

***[57] in "Mason Wikipédia" (http://en.wikipedia.org/wiki/Mason_%28Perl%29)***

***[58] in "Mason HQ" (http://www.masonhq.com/docs/manual/Mason.html)***

***[59] in "Apache Wikipédia" (http://en.wikipedia.org/wiki/Apache_HTTP_Server)***

***[60] in "Chroot Wikipédia" (http://en.wikipedia.org/wiki/Chroot)***

***[61] in "AJAX Tutorial" (http://www.w3schools.com/ajax/ajax_httprequest.asp )***

# Anexo 1 Conceptualização

O estudo efectuado durante a fase de conceptualização desde s*oftware*, levou ao desenvolvimento de algumas ideias condutor – deste projecto. Foi efectuada uma previsão do tipo de funcionalidades e aspecto geral que esta aplicações HTTP deveria ter. A inserção deste estudo de conceptualização neste anexo, permite mostrar as *guide lines* ou linhas direccionais de evolução ao projecto. Este estudo, além de útil para o desenvolvimento do projecto, resultou no aproveitamento destas ideias e conceitos.

Em termos de aspecto o serviço deveria apresentar os seguintes componentes:

- Página de Entrada/Autenticação;
- Página Inicial;
- Menu Equipamentos;
- Menu Utilizadores;
- Menu Serviços;

Página de Entrada/Autenticação

Esta é a primeira página a aparecer ao utilizador. Permite ao utilizador identificar-se e inicia uma sessão segura em SSL.


Figura 109 - Página de Entrada/Autenticação

Deve ser utilizada a abordagem AJAX para comunicar com o servidor e determinar se o *username* e a *password* são válidos no sistema.

Página Inicial

Esta página é a primeira a ser vista pelo utilizador após a entrada no sistema. Deverá apresentar as configurações determinadas por este de forma a tornar o *site* mais prático. Deverá detectar qual o utilizador que efectuou a autenticação e apresentar a página com as suas configurações (língua, cor, nome, opções iniciais)

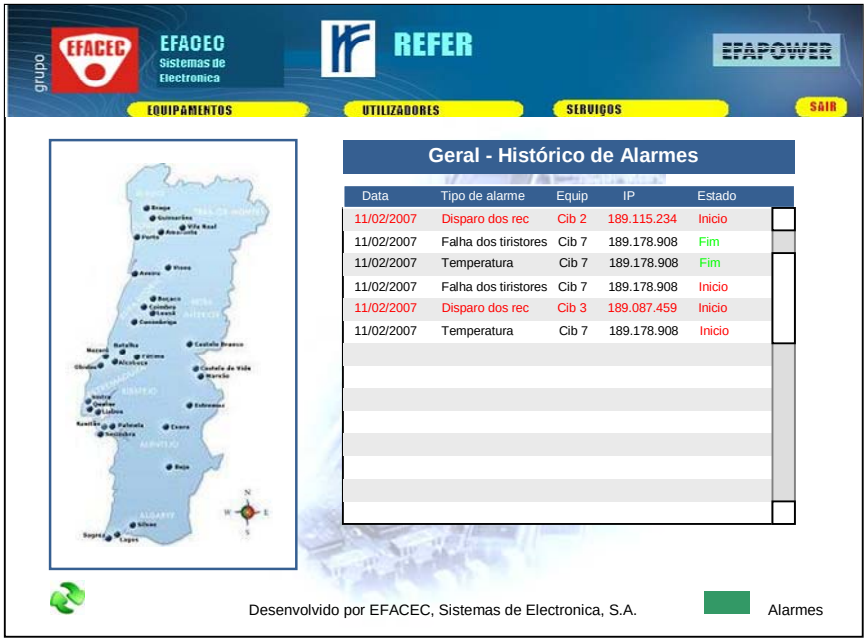


Figura 110 – Página Inicial do servidor *Web*

Opções Iniciais

O ecrã fica dividido em dois *frames* diferentes, podendo o utilizador configurar o que deseja que apareça por defeito em cada *frame*, facilitando assim a visualização do sistema ou de um determinado equipamento de cada vez que o utilizador acede ao sistema. Exemplo de opções para a página Inicial:

- Informação de um equipamento;
- Mapa dos grupos (geral);
- Mapa de equipamentos (específico);
- Árvore de grupos;
- Últimos acessos;
- Histórico de alarmes (de um equipamento, grupo de equipamentos ou geral);

No canto inferior direito aparecerá um ícone ou imagem sugestiva do estado dos alarmes do sistema. Se estiver a verde não existirão alarmes no sistema. Se estiver a vermelho ou intermitente indica a existência de um alarme. Clicando sobre o ícone deverá ser possível aceder a informação detalhada sobre o alarme.

Poderá reproduzir um som sempre que um alarme estiver activo, fornecendo uma outra forma de alerta. No mapa dos equipamentos deverá aparecer sinalizado a vermelho ou intermitente o equipamento ou grupo com o alarme activo.

Passando o rato sobre as opções presentes na barra inicial (Equipamentos, Utilizadores e Serviços) aparecerá um menu do estilo *drop-down* com as opções disponíveis para cada menu.

No canto superior direito existirá ainda um botão SAIR ou LOGOUT para sair da sessão e regressar ao ecrã inicial (página de autenticação).

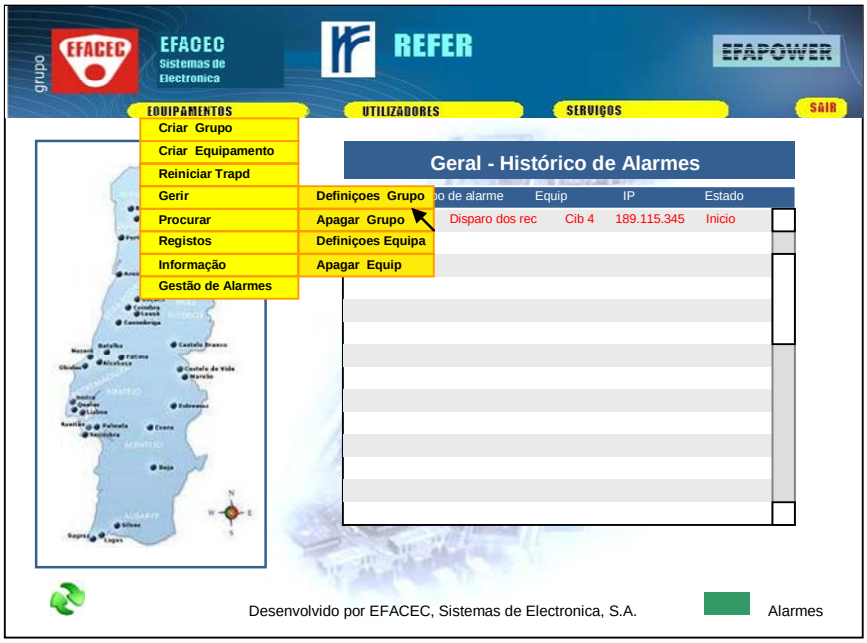


Figura 111 – Opções do menu

Cada menu terá as seguintes opções:

<u>Equipamentos:</u>

- Criar Grupo;

- Criar Equipamento;
- Reiniciar *trapd*;
- Gerir;
- Procurar;
- Registos;
- Informação;
- Gestão de Alarmes;

Utilizadores:

- Listar;
- Criar Utilizador;
- Criar Grupo;
- Gerir;
- Privilégios;
- *Password*;
- Procurar;

Serviços:

- Página Inicial;
- *Upload* de Ficheiros;
- Configuração do Servidor;
- Configuração da Página Inicial;

- Registo de Medidas;
- Informação sobre Servidor;
- Mapa Geral;
- Árvore de Grupos;
- Menu Equipamento

Criar Grupo

No menu "Criar Grupos" deverá ser possível definir onde se deseja criar o subgrupo. Deverá igualmente ser possível definir o nome ao grupo, dar uma breve descrição do mesmo e introduzir as coordenadas da localização do equipamento (ou apontar com o rato no mapa).


Figura 112 – Menu Criar Grupo

Criar Equipamento

Poderemos definir o nome do equipamento, a sua localização (coordenadas ou apontando no mapa), o IP, Porto para comunicação, TagID, se é *Foward* ou *Gatex*, o *email* para onde deverão ser enviados os alertas de alarme e o tipo de equipamento.

Nesta última opção poderá surgir uma lista com *scroll* com as várias opções de equipamentos disponíveis.


Figura 113 – Menu Criar Equipamento

Na definição das localizações ou do tipo de equipamento pode surgir uma barra estilo *drop-down* com as várias opções disponíveis (estilo Google Suggest) ou com *scroll* para as várias opções. A utilização de AJAX poderá ser vital para facilitar de introdução de dados.

Reiniciar *Trapd*

Deverá surgir um *pop-up* após seleccionar esta opção perguntando ao utilizador se deseja prosseguir com o comando. Esta opção dará ao utilizador a hipótese de cancelar a sua anterior ordem.

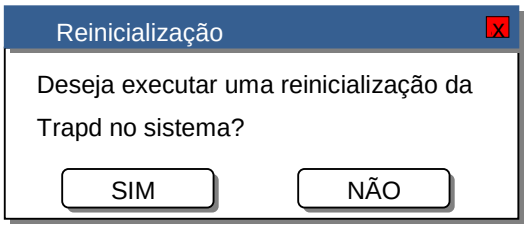


Figura 114 – *Pop-up Trapd*

Gerir

No menu "Gerir" deverá ser possível:

- Modificar as definições de um Equipamento;
- Apagar um Equipamento;
- Modificar as definições de um Grupo;
- Apagar um Grupo;
- Modificar parâmetro;

Na opção modificar parâmetro deverá ser possível modificar um parâmetro de um equipamento específico ou de um grupo de equipamentos. Este passo torna possível a alteração em simultâneo de valores e parâmetros de vários equipamentos.


Figura 115 – Menu Gerir


Figura 116 – Definição de parâmetros

## Procurar

Neste menu será possível definir parâmetros para pesquisa de um equipamento. Esta pesquisa é particularmente útil em sistemas com muitos

equipamentos sob supervisão. Em vez de procurar na Árvore de Grupos ou no Mapa, a pesquisa através deste método é mais rápida e directa.

Neste menu são requeridos os parâmetros:

- Nome;
- Grupo;
- IP;
- Localização;
- *Tag*;


Figura 117 – Menu Pesquisa

Registos

No menu registos aparecerá um submenu com as seguintes opções “Por Equipamento”, “Por Grupo” e “Geral”.


Figura 118 – Menu Registos

*Por Equipamento:*

- Mostra histórico de registo de alarmes ou falhas de equipamentos (base de dados);
- Regista o início e fim de cada alarme;
- Regista os alarmes activos a vermelho e os não activos a negro (cor normal);
- Tabela organizada cronologicamente.

Clicando sobre um alarme, acedemos a informação detalhada sobre o mesmo (que operador verificou/solucionou o problema, data de resolução, comandos automáticos configurados).

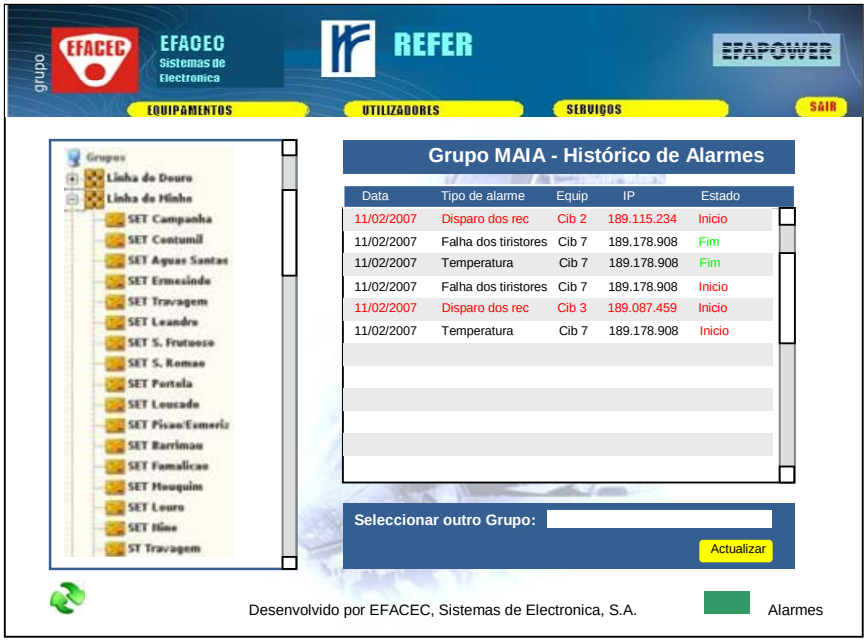


Figura 119 – Histórico de Grupos

*Por Grupo:*

Mesmos conceito que a tabela para equipamentos, com a excepção que aparecem todos os alarmes de todos os equipamentos de um grupo.

*Geral:*

Mesmos conceito que a tabela para equipamentos, com a excepção que aparecem todos os alarmes de todos os equipamentos da rede.

Menu Informação

Neste menu, organizado em *frames*, aparece um *frame* do lado esquerdo com um mapa da região/grupo em que se insere o equipamento ou uma árvore de grupos para uma melhor navegação entre grupos. No *frame* direito aparecerá uma imagem do equipamento (imagem correspondente a cada equipamento). Aparecerá um sinóptico com os componentes do sistema, fornecendo uma informação visual acerca de estados e medidas.

Clicando sobre o nome do equipamento, deverá ser possível redireccionar para a hiperligação do servidor *Web* do SNMP (presente nos CIB). Deverá apresentar também um *frame* com os alarmes activos do equipamento. Do lado direito aparecerá um menu semelhante ao menu disponível na página do Efapower SNMP WebServer.

Para a actualização destes valores, a aplicação *Web* enviará pedidos de actualizações do componente directamente para o Módulo de Comunicações.

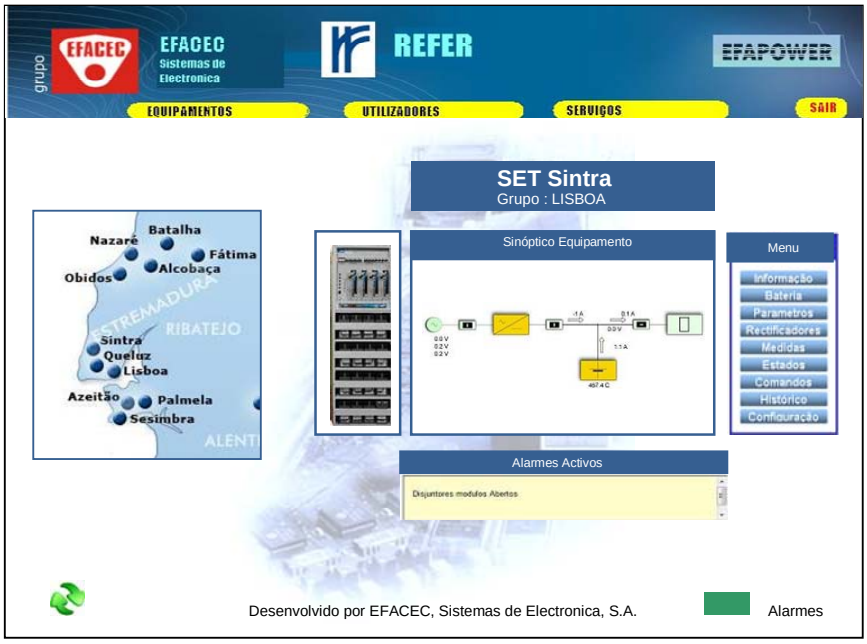


Figura 120 – Informação sobre equipamento

Gestão de Alarmes

Na Gestão de Alarmes o operador poderá definir prioridades de alarmes, activar ou desactivar alarmes, configurar as acções automáticas do Servidor *Web* e configurar endereços de *email* e GSM.

Nos botões de acção deverá ser possível pressionar o botão de cancelamento para desactivar o alarme activo (útil quando temos vários alarmes activos e o operador já tomou conhecimento deste alarme).

O processo inverso também é possível, tornando o alarme de novo activo (esta situação só é possível se o alarme estiver de facto activo).


Figura 121 – Gestão de Alarmes

Nas configurações automáticas aparecerá uma tabela (com *scroll*) de todos os alarmes possíveis (definidos por prioridade). Clicando sobre um alarme, surge um conjunto de acções possíveis de configurar automaticamente para o alarme (desactivar CIB, Reiniciar PSM, desactivar rectificador, *etc*.).


Figura 122 – Comandos automáticos

Os comandos que forem activados serão automaticamente executados quando um alarme deste tipo for detectado. Desta forma, pretende-se dar uma resposta mais rápida a um alarme até à chegada de um técnico para resolver a avaria.

No menu Configurar Alertas será possível definir o endereço de *email*, de telemóvel e até mensagens pré definidas para enviar ao operador.

No menu de definição de prioridades será possível definir que tipo de alarme tem a prioridade mais elevada ou que tipo de equipamento que é o mais importante.

Menu Utilizadores

O menu Utilizadores apresenta como submenu:

- Listar;
- Criar Utilizador;
- Criar Grupo;
- Gerir;

- Privilégios;
- *Password*;
- Procurar;
- Registos.

Listar

Este menu permite a apresentação de uma árvore de grupos com o conjunto de utilizadores e de uma tabela com os vários utilizadores registados no sistema.

Nesta tabela deverão constar as seguintes informações de cada utilizador:

- Identificador;
- Utilizador (*username*);
- Nome;
- Privilégios;

Estes dados serão obtidos da Base de Dados do sistema.


Figura 123 – Listar Utilizadores

Criar Utilizador

No menu de criação de utilizador deverão constar campos como *username*, nome, *password*, *email*, telefone, telemóvel, empresa, identificação, cargo, tipo, informações e idioma.


Figura 124 – Criar Utilizador

Criar Grupo

No menu de criação de grupos deverão ser apresentadas as opções:

- Nome;
- Descrição;
- Privilégios;

Em termos de aparência deverá ser semelhante à página anterior.

Privilégios

Deverão surgir duas opções principais: por grupos ou por equipamento. A partir desta opção o utilizador deverá ser redireccionado para uma página com o seguinte aspecto:


Figura 125 – Gestão de privilégios

O botão Criar Grupo permitirá criar um novo grupo e atribuir um nível de privilégio. Clicando sobre o botão apagar, poder-se-á eliminar um grupo. Clicando sobre o acesso, poder-se-á modificar o nível de privilégio para o grupo.

*Password*

Nesta página deve ser possível ao cliente alterar a sua *password* corrente. O administrador do sistema poderá alterar todas as senhas dos restantes utilizadores do sistema, bastando-lhe aceder a ***Utilizadores*** > ***Gerir***.


Figura 126 – Alteração da *password*

Procurar

Nesta página será possível pesquisar um utilizador específico do sistema para ter acesso à sua informação. Para tal serão disponibilizados três campos de pesquisa: *Username*, Nome ou Identificação. Em alternativa à introdução de dados, poderá surgir uma tabela com os vários nomes e identificações presentes no sistema para que o utilizador encontre quem procura.

Gerir

Este menu de administração redireccionará para um menu com três opções:

- Gerir Perfis;
- Gerir Grupos;
- Gerir Privilégios;

Na gestão de Perfis temos uma lista com todos os utilizadores do sistema (semelhante ao menu Listar mas com a opção de apagar). Clicando sobre um

utilizador, ter-se-á acesso a todos os campos da sua informação (tal como no menu Criar Utilizador). Será possível alterar as suas definições e guardar o utilizador.

Na gestão de grupos será possível definir quem é que faz parte de cada grupo, através de uma caixa de selecção:

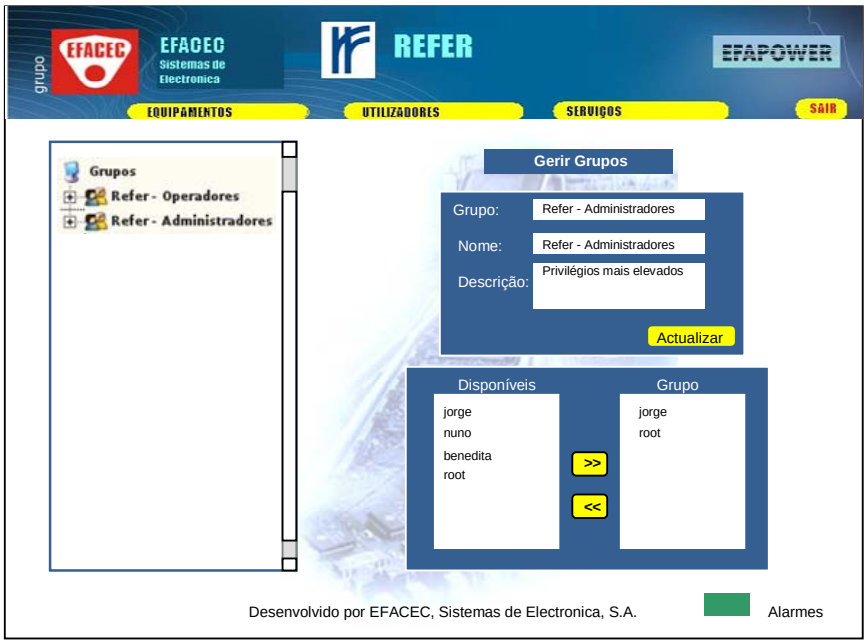


Figura 127 – Gestão de grupos de utilizadores

Na gestão de privilégios é possível definir a que podem aceder utilizadores de determinados grupos. Ou seja, é possível configurar os níveis de acesso. A utilização de *checkbox* para definir o que está acessível ou não facilita o processo de gestão.

Registos

Neste menu aparecerão tabelados todos os registos de acesso ao sistema dos utilizadores registados e não registados. Cada registo conterá o Nome (*username*), Estado (*LOGIN/LOGOUT*), informação (*OK/ERROR* ou ACEITE/NÃO ACEITE), data e IP de acesso. Na lateral existirão dois campos que permitirão definir uma data para o inicio da tabela e uma data para o fim, situando-a assim num período de tempo definido.

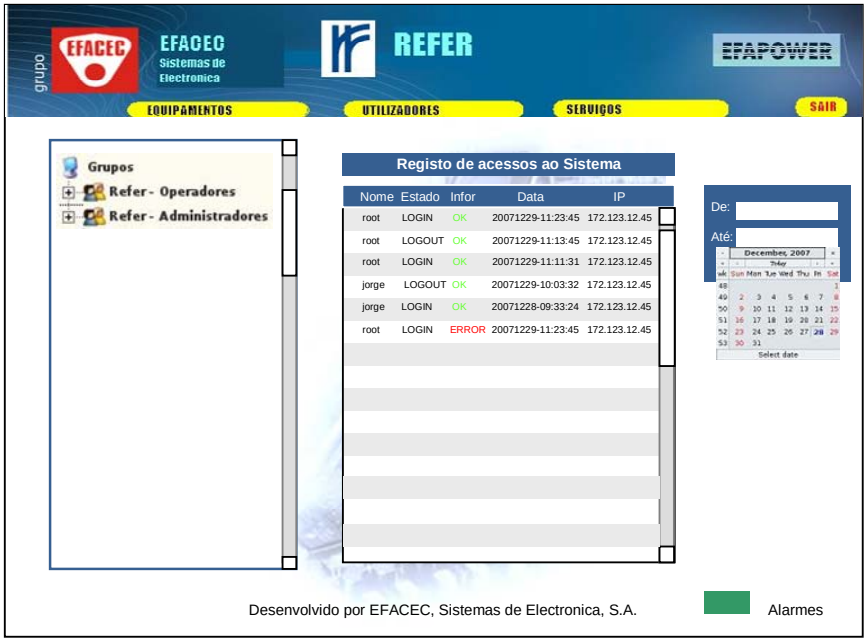


Figura 128 – Registo de Utilizadores

Menu Serviços

O menu de serviços incluí:

- Página Inicial;
- *Upload* de Ficheiros;
- Configuração da Página Inicial;
- Registo de Medidas;
- Informação sobre servidor;
- Mapa Geral;
- Árvore de grupos;
- Configurador de Sinóptico.

<u>Página Inicial</u>

Ao clicar nesta opção, o utilizador abrirá a página inicial da aplicação *Web*. A definição desta página inicial será feita em "Configuração da Página Inicial".

Carregamento de Ficheiros

Neste menu será possível efectuar o *upload* para o servidor de vários tipos de ficheiros diferentes. Pode ser feito o *upload* de um logótipo da empresa do cliente, da imagem dos equipamentos, de um novo sinóptico ou de um ficheiro de base de dados (configurações, *etc*.).


Figura 129 – *Upload* de ficheiros

O carregamento de ficheiros deverá ser executado via .PHP ou .ASP e deverá ter uma imagem de previsão, para que o utilizador saiba qual a imagem actual e qual a que a irá substituir.

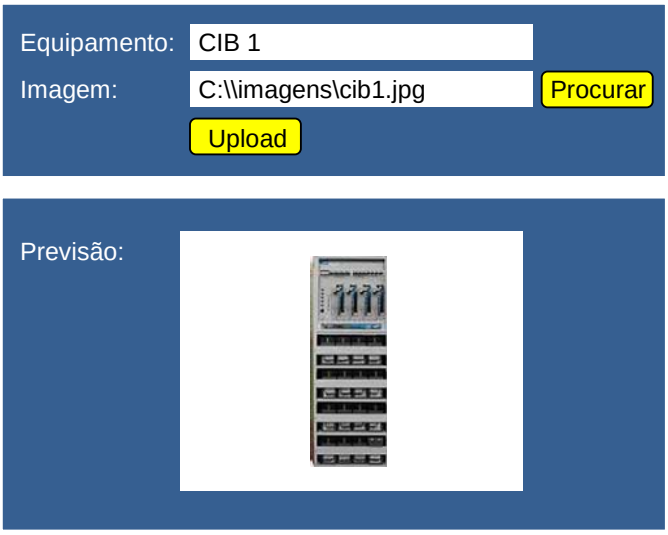


Figura 130 – Previsão de ficheiro

O tamanho permitido para a imagem do logótipo do cliente assim como dos equipamentos ficará limitado internamente para evitar carregar um ficheiro demasiado "pesado" para ser aberto numa página de HTML. O *upload* da base de dados está limitado ao tamanho normal de um ficheiro de exportação de base de dados. Os tipos de ficheiro de base de dados importáveis resumem-se a ficheiros de configurações da aplicação *Web* e dos equipamentos de rede, dados dos utilizadores e dos equipamentos.

Configuração do Servidor

Neste menu podem-se definir algumas características do servidor, tais como:

- Idioma por omissão;
- Página Inicial por omissão;
- Inserir o Nome do Cliente.

Configuração da página Inicial

Neste menu é possível configurar os dois *frames* da página inicial e o idioma para o utilizador actual. Deverão aparecer três campos para serem preenchidos:

- Idioma;
- *Frame* Esquerdo;
- *Frame* Direito;

Para cada um dos *frames* deverão existir as seguintes opções:

- Mapa Geral;
- Árvore de Grupos de Equipamentos;
- Árvore de Grupos de Utilizadores;
- Histórico de alarmes;
- Histórico de Acessos ao sistema;
- Mapa Grupo 1;
- Mapa Grupo 2;
- Mapa Grupo N;

Estas definições são guardadas para que, da próxima vez que o utilizador aceder ao *webserver*, os *frames* e o idioma estejam configurados conforme as necessidades deste. Esta funcionalidade torna o sistema mais prático e personalizável.

Registo de Medidas

Nesta opção é possível definir uma data de início e fim de recolha de dados e conjunto de dados para um equipamento. Poderão ser lançados até quatro pedidos de dados em simultâneo.

Sempre que o servidor lança um destes processos, vai fazer *polling* de determinados dados a um determinado equipamento durante um período de tempo que se pode estender a meses. O número e tipo de medidas recolhidas estarão limitados pelo tamanho e capacidade da base de dados.

Os dados não estarão disponíveis durante a recolha, sendo no final do período estipulado para a recolha enviado um *email* a avisar da conclusão da mesma. Estes dados serão apresentados sob a forma de uma tabela, sendo possível exportá-los num formato interpretável (folha de dados EXCEL, XML ou base de dados MDB).

Poderá ser utilizado um componente para produzir um gráfico a partir dos dados presentes na base de dados.


Figura 131 – Registo de Medidas

Existem quatro campos, cada um com:

- Equipamentos;
- Medidas;
- De (data);

- Até (data);
- Nome (a ser atribuído à recolha).

Na parte posterior da página inicial aparece um *frame* com informação relativa aos processos de recolha de informação activos.

- Sem Pedidos (Não há qualquer processo a recolher dados);
- Em Aquisição (Há um processo a recolher dados);
- Recolha Terminada (Há um processo que terminou a sua recolha);

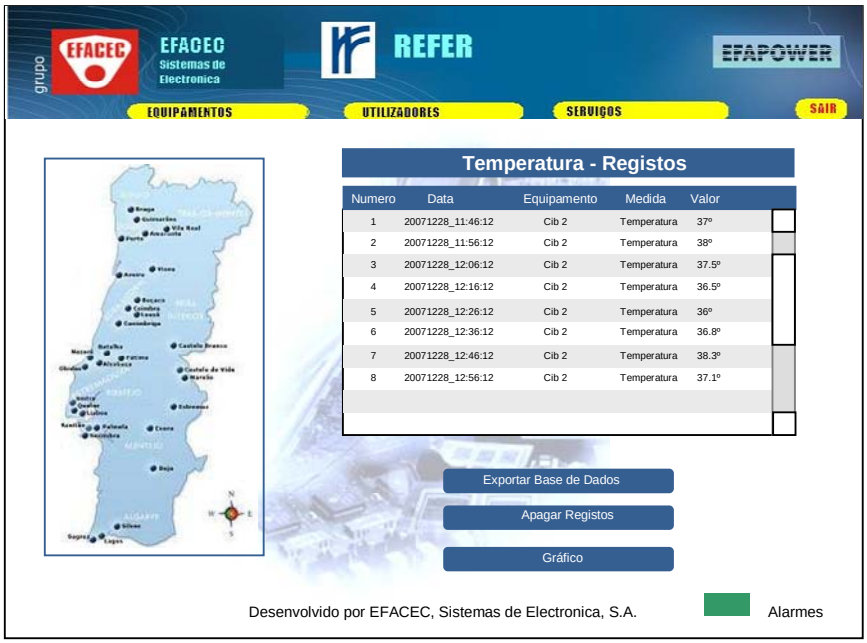


Figura 132 – Tabela de registos

<u>Informações sobre o servidor</u>

Neste menu são apresentados um conjunto de informação relativas ao servidor, tais como:

Versão:

- Base de Dados;

- IP;
- Nome do Fabricante;
- Número de Equipamentos Conectados à rede;
- Número de Grupo definidos.

Mapa Geral

Esta opção apresenta o mapa geral com cada grupo de equipamentos. Se um equipamento começa a funcionar incorrectamente, o seu símbolo muda a cor para vermelho. Desta forma temos uma rápida referência visual ao estado de cada equipamento.

Árvore de Equipamentos

A árvore de equipamentos é uma representação gráfica dos vários grupos existentes no sistema, com os respectivos elementos. É possível navegar entre estes, seleccionando-os.

Configurador de Sinóptico

No menu de configuração de sinóptico será possível escolher entre vários esquemas de sinópticos disponíveis e configurar os elementos constituintes de um determinado sinóptico.

*System Keeper*

A redundância do sistema deverá ser assegurada por um módulo externo que assegure o correcto funcionamento de todo o sistema. Este módulo, denominado *system keeper* permitirá manter o correcto funcionamento de todos os módulos do sistema. Funcionará como um *watchdog*, verificando regularmente se os PID dos processos se encontram ainda activos, e, no caso de um se ter desactivado, reiniciar o módulo.

Deverá ser ainda responsável pela manutenção da base de dados, gerindo os dados de uma base de dados gémea no sistema que, no caso de falha ou erro da principal, é activada.

Este sistema permite uma gestão eficaz do sistema e salvaguarda dos dados e da gestão do mesmo.

**Módulo Gestão Regional**

Um módulo adicional a desenvolver é o módulo de gestão regional que permita a comunicação entre diferentes sistemas de monitorização distribuída. O objectivo é que através da partilha das bases de dados de cada um possam passar a gerir apenas uma determinada região.

Este sistema toma conhecimento de um outro Efapower WebServer a monitorizar a rede e, através de um protocolo definido por um administrador de rede, define uma região para monitorização, "oferecendo" os dados dos equipamentos dessa região ao outro sistema quando solicitado.

Desta forma, em grandes extensões de território e com vários sistemas deste tipo distribuídos, é possível gerir a rede sem sobrecarregar a mesma de pedidos de *polling*. Um sistema gere a rede que lhe foi atribuída e disponibiliza o acesso à base de dados remotamente para sistemas distantes.

A troca de informações pode-se efectuar através um porto definido utilizando *sockets* TCP através de TCP/IP.

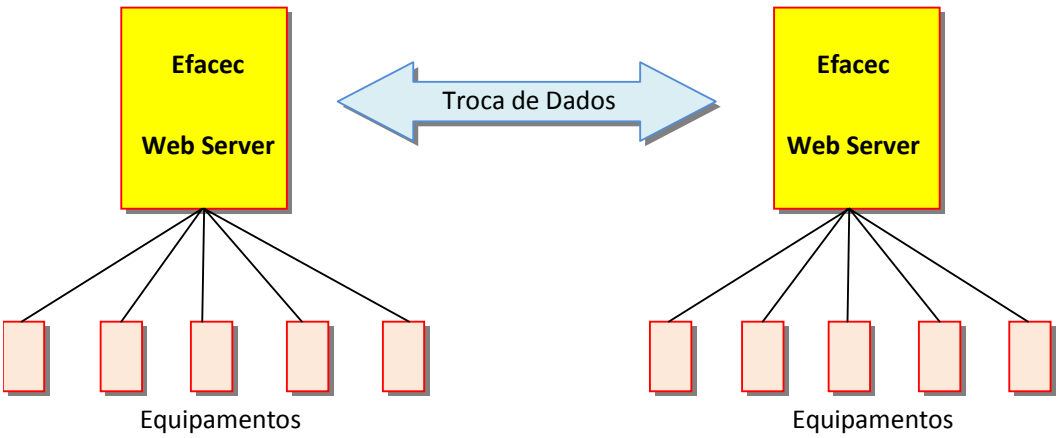


Figura 133 – Troca de dados entre sistemas EFACEC Webserver

# Anexo 2 Cronograma do Projecto

Tabela 8 – Cronograma

| *Cronograma* | *Semana* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
| Estudo do Estado de Arte | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Elaboração de Requisitos | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Definição de Modelo Final | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Interface para utilizador | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Base de Dados | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Comunicação por Modem | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Comunicação por Ethernet | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Gestão de Alarmes | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Testes e Depuração | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tese/Dissertação | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |