



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

BACHARELADO EM ENGENHARIA DA COMPUTAÇÃO

GUSTAVO LUIZ BENEVIDES DE OLIVEIRA

**DESENVOLVIMENTO DE SISTEMA SUPERVISÓRIO PARA CONTROLE DE
ACESSO ATRAVÉS DO CLP**

RECIFE

2015

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

GUSTAVO LUIZ BENEVIDES DE OLIVEIRA

**DESENVOLVIMENTO DE SISTEMA SUPERVISÓRIO PARA CONTROLE DE
ACESSO ATRAVÉS DO CLP**

Trabalho de graduação apresentada no Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para a obtenção do grau de Bacharel em Engenharia da Computação.

Orientador: Prof. Dr. Geraldo Leite Maia

RECIFE
2015

GUSTAVO LUIZ BENEVIDES

**DESENVOLVIMENTO DE SISTEMA SUPERVISÓRIO PARA CONTROLE DE
ACESSO ATRAVÉS DO CLP**

TRABALHO DE GRADUAÇÃO

Trabalho de Graduação apresentado à graduação em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco para obtenção do grau de Bacharel em Engenharia da Computação.

APRESENTAÇÃO em

Recife, _____ de _____ de 2015.

BANCA EXAMINADORA

Orientador: Prof. Dr. Geraldo Leite Maia

1º Avaliador: Prof. Aluizio Araújo

2º Avaliador: Odilon Maroja

Recife

2015

AGRADECIMENTOS

A Deus que me deu forças e perseverança para concluir esta etapa difícil que foi o curso de graduação em Engenharia.

A minha família por me dar todo o apoio, desde a minha educação básica às condições de poder concluir esta faculdade de forma consistente.

Aos meus verdadeiros amigos por se interessarem na carreira que eu escolhi e por se demonstrarem sempre dispostos a me auxiliar.

Ao meu sócio Humberto por sempre me apoiar e segurar a empresa nos momentos de dedicação à Faculdade.

Ao professor Geraldo Leite Maia por me introduzir e me orientar em um projeto tão interessante, aumentando ainda mais a minha paixão pelo ramo da elétrica e automação.

Ao professor Aluizio Araújo por se disponibilizar a ser avaliador deste trabalho.

Aos professores Odilon Maroja, Carlos Alexandre e Hélio Magalhães, por sempre se demonstrarem tão dispostos a ajudar e se esforçarem para que nós alunos pudéssemos nos tornar Engenheiros capacitados para o mercado.

RESUMO

Este trabalho leva em conta a evolução tecnológica que revolucionou os processos industriais nos últimos anos. Devido à necessidade de melhora na qualidade dos equipamentos presentes nas indústrias e uma maior segurança para todos os funcionários, é cada vez mais importante o controle efetivo de acesso de todos os colaboradores no ambiente industrial, visando sempre sua segurança e bem-estar. Para isto ocorrer, é necessário um sistema de controle tão confiável quanto, que possa armazenar as informações da melhor maneira possível e que possa se integrar com os sistemas já presentes da forma mais fácil também, bem como uma manutenção mais rápida e prática.

Palavras-chave:

Automação Industrial. Sistemas Supervisórios. Controle De Acesso. Controlador Lógico Programável (Clp). Redes Industriais

LISTA DE FIGURAS

FIGURA 1 CONFIGURAÇÃO DO DRIVER DE COMUNICAÇÃO MODBUS.....	15
FIGURA 2 TELA DE REMOÇÃO DE USUÁRIOS	18
FIGURA 3 EDIÇÃO DE DADOS DOS USUÁRIOS	19
FIGURA 4 ARQUITETURA DE UMA REDE MODBUS.....	20
FIGURA 5 FRAME DE MENSAGEM ASCII	21
FIGURA 6 FRAME DE MENSAGEM RTU	22
FIGURA 7 FRAME MODBUS TCP	23
FIGURA 8 CONFIGURAÇÃO DE REGISTRADOR_BASE_SENHAS	24
FIGURA 9 CRIAÇÃO DA TABELA DADOS_USUÁRIO	27
FIGURA 10 CRIAÇÃO DE TABELA ESTATÍSTICAS.....	28
FIGURA 11 CRIAÇÃO DO ODBC SCADA.....	29

SUMÁRIO

1	INTRODUÇÃO	8
1.1	CONTEXTO	8
1.2	MOTIVAÇÕES E OBJETIVOS	9
1.3	METODOLOGIA E FERRAMENTAS	10
1.4	ORGANIZAÇÃO DO TRABALHO	12
2	SISTEMAS SUPERVISÓRIOS	13
2.1	SQL SERVER	13
2.2	COMUNICAÇÃO MODBUS	14
2.3	CADASTRO E SENHAS	16
2.4	REMOÇÃO	18
2.5	EDIÇÃO	19
3	MODBUS	20
3.1	MODBUS SERIAL	21
3.2	MODBUS PLUS	22
3.3	MODBUS TCP	22
3.4	APLICAÇÃO	23
5	SQL SERVER	26
5.1	INSTALAÇÃO DO SQL SERVER	26
5.2	INSTALAÇÃO DO SQL MANAGEMENT STUDIO	26
5.3	CRIAÇÃO DE TABELAS	27
5.3.1	Dados_Usuário	27
5.3.2	Estatísticas	28
5.5	ODBC	29
6	CONSIDERAÇÕES FINAIS	30
	REFERÊNCIAS	31

1 INTRODUÇÃO

1.1 CONTEXTO

Em meados do século XVIII, deu-se início à Revolução Industrial na Inglaterra, fato que contribuiu para a aceleração do processo de fabricação de produtos diversos, antes feitos de forma artesanal.

A Revolução Industrial estabeleceu um marco transitório de uma sociedade predominantemente agrícola e organizada na produção de bens de consumo de forma artesanal, para uma sociedade, industrialmente, mais produtiva, voltada ao consumo e organizada dentro de um novo modelo econômico de sucesso financeiro, associando as novas técnicas contábeis ao mercado de capitais [1].

Para atingir um elevado nível de produção, os principais fatores como velocidade e eficiência são limitados quando se trata de mão de obra humana. Logo, a máquina vem, ao longo dos anos, substituindo o trabalho humano no processo fabril para suprir o aumento da demanda decorrente do processo natural do crescimento populacional [2].

No processo de automatização, a máquina deve ser capaz de cumprir tarefas baseadas em decisões, que são tomadas em função de sinais de várias naturezas, que provêm de todo o sistema controlado. Estes sinais muitas vezes provêm de sensores, os quais tem o papel de substituir os próprios órgãos sensoriais humanos (visão, audição, tato...). Neste cenário, o sistema de controle é o cérebro do processo, responsável por toda a inteligência e lógica da planta fabril.

Com o desenvolvimento dos microprocessadores em larga escala em 1972, o equipamento (hardware) analógico vem sendo substituído pelo digital. Todos os tipos de controladores vêm sendo substituídos pela tecnologia digital. Já o trabalho do computador, atuando como supervisor de um processo, fornece informações para o operador e executa funções para a determinação de referências operacionais para a instrumentação analógica. No fim da década de 1960, chegam os microcomputadores, máquinas mais baratas e mais adequadas às indústrias de pequeno e médio portes. O aumento da produção é caracterizado pelo aumento da confiabilidade e pela flexibilização introduzida com a progressiva padronização de linguagens de

programação desenvolvidas para os computadores, conhecidas como softwares de programação [1].

Com a tecnologia evoluindo de maneira exponencial, os processos industriais passaram cada vez mais a se tornar automatizados, substituindo parte da mão de obra que realizava trabalhos mecânicos. Uma nova etapa surgiu na revolução industrial, e ao passo que a automação era implementada, os trabalhadores passaram a realizar supervisão dos processos industriais. A partir disto foi identificada uma nova necessidade no mercado: Uma interface eficiente para os novos supervisores e um controle de acesso para os funcionários das fábricas.

1.2 MOTIVAÇÕES E OBJETIVOS

Devido a um controle cada vez mais rígido dos órgãos governamentais de supervisão, as empresas estão investindo em sistemas digitais que realizem tais tarefas. O ponto digital é um dos mais utilizados em organizações no geral, e sabe-se que funciona muito bem para o que foi projetado: escritórios com baixa emissão de poluentes e ambientes pouco agressivos, com umidade regular e pouca sujeira.

A evolução da tecnologia e dos microprocessadores beneficiou diretamente as tecnologias de automação, permitindo que equipamentos cada vez mais modernos pudessem operar nas fábricas. Além dos CLPs, utilizados para controle dos processos, foram incorporadas também as Interfaces Humano Máquina (IHM), utilizadas para substituir antigos painéis de operação, estas interfaces dotadas de tela gráfica colorida, teclado/mouse/touchscreen conferem ao sistema melhores condições para o controle e supervisão do extenso número de variáveis existentes num processo produtivo [1].

As telas do tipo touchscreen constam nas IHMs mais modernas, e são projetadas para suportar as condições mais severas dos ambientes industriais, como temperatura, umidade, calor e poeira. Considerando estes fatores, ainda se leva em conta que estes dispositivos podem se comunicar em rede com outros equipamentos de automação, o que facilita a leitura e controle de toda a informação gerada, assim sendo um elemento mais adequado para o controle de acesso em ambientes industriais.

Atualmente, as indústrias fazem um grande uso de computadores com Sistemas Supervisórios para sua planta, pois estes são capazes de realizar controle do processo, monitorar os status dos elementos, exibir análises gráficas e estatísticas, alertar sobre falhas, erros e muito mais funcionalidades para melhorar o trabalho tanto dos operadores quanto dos analistas de produção. Estas mesmas possibilidades podem ser aplicadas ao controle de acesso dos trabalhadores, permitindo que os responsáveis pelo Departamento Pessoal possam ter acesso à diversas informações que venham a melhorar também o seu trabalho.

Seguindo esta idéia, esse trabalho tem o foco de implementar uma melhora no controle de acesso em ambientes industriais, através das mesmas tecnologias utilizadas nos processos de automação. O contexto a ser aplicado neste caso será o acesso ao laboratório do Departamento de Engenharia Elétrica da UFPE, no entanto, utilizando todos os conceitos de um sistema de automação industrial, para assim simular o mesmo ambiente de uma fábrica.

1.3 METODOLOGIA E FERRAMENTAS

O Capítulo corrente tem como função apresentar um resumo de todas as ferramentas e metodologias utilizadas neste trabalho de graduação. Começamos descrevendo sobre os sistemas SCADA e a sua ferramenta utilizada, Elipse. Em seguida, será utilizada a referência [3] para dar uma breve introdução ao protocolo de Redes Industriais Modbus, passando para a ferramenta SQL Server, banco de dados utilizado para este projeto. Por fim, faremos uma breve introdução sobre CLPs, se baseando na referência [4].

- **Sistemas Supervisórios - Elipse SCADA:** Na maioria dos processos de produção industrial não é possível ter uma boa noção e controle do que está sendo produzido apenas observando o maquinário. Quando isto é possível, quase nunca se tem um controle preciso daquilo que está sendo produzido, pois tudo acaba dependendo de um controle manual. Os sistemas supervisórios vieram para sanar este problema. Por meio da visualização gráfica em cores e com alta definição, torna-se muito

mais prático e rápido ao operador obter informações precisas a respeito do status do processo [1]. Estes tipos de sistema suportam níveis de usuário para controle de acesso, permitindo assim que diferentes usuários possam ter diversas atribuições. A ferramenta escolhida para esta função foi o Elipse Scada (*Supervisory Control and Data Acquisition*).

- **Redes Industriais – Modbus:** A necessidade de exportar dados do processo local para pontos distantes, seja por questões de segurança ou de redução do custo operacional, seja simplesmente por comodidade ou simplificação no processo, levou à criação das redes industriais. Elas garantem a transmissão de informações relativas ao processo, de maneira rápida, em ambiente eletromagneticamente ruidoso, entre dois ou mais pontos [5]. Diversos são os protocolos de comunicação utilizados na indústria. Pode-se dizer que um protocolo de comunicação é um idioma no qual dois ou mais equipamentos conversam. Fazendo uma analogia para melhor entendimento, uma pessoa que fala apenas em português não consegue conversar com outra que fale em russo. O mesmo ocorre com CLPs que trabalham com protocolos de comunicação diferentes [5]. O protocolo Modbus foi o escolhido para este trabalho devido à sua praticidade e pelo fato de a maioria dos equipamentos atuais darem suporte a este tipo de comunicação.
- **Banco de Dados – SQL Server:** O sistema supervisório terá diversas informações que terão que ser armazenadas em um ambiente confiável e de fácil acesso. Para isto, foi escolhido o banco de dados SQL Server e utilizada a ferramenta SQL Management Studio para gerenciar o banco de dados. Após criado o ODBC, a ferramenta Elipse SCADA foi devidamente configurada para a comunicação efetiva com o banco de dados SQL, podendo assim ler, apagar e escrever registros no mesmo.

- **Controlador Lógico Programável – TPW03:** A estrutura física do CLP é um conjunto de circuitos eletrônicos interligados formados por processadores, memórias, barramentos, dispositivos de entrada e saída, fonte de alimentação e terminal de programação [5]. Este dispositivo funciona como o cérebro de qualquer máquina. Ele recebe os sinais dos sensores como entrada, e em função disto gera as saídas que ativam os atuadores, sendo considerado um sistema com re-alimentação. Os programas do CLP, na maioria das vezes feitos em LADDER, são feitos em um computador e carregados através de um cabo de comunicação.

1.4 ORGANIZAÇÃO DO TRABALHO

O capítulo 2 está organizado com foco nos Sistemas Supervisórios e na ferramenta Elipse Scada, por ser a principal ferramenta do projeto, onde quase tudo se concentra. Assim, são apresentadas suas funcionalidades e características principais, além de como foram configuradas todas as opções possíveis que permitam comunicação com as outras ferramentas do trabalho.

O capítulo 3 tratará de Redes Industriais, dando uma breve introdução sobre como elas funcionam e atuam para assim poder ser abordado o protocolo de comunicação Modbus, como ele é estruturado para se comunicar com os outros equipamentos e quais suas funcionalidades, vantagens e desvantagens para um projeto.

No capítulo 4 será abordado brevemente o banco de dados SQL server, focando em sua comunicação com o SCADA e porque foi escolhido para este trabalho.

Por fim, no capítulo 5, são feitas as considerações finais e discutidas as dificuldades encontradas durante a criação, simulação e testes realizados. Além disso, são apresentadas algumas sugestões de trabalhos futuros que poderiam dar continuidade a este trabalho.

2 SISTEMAS SUPERVISÓRIOS

Os sistemas supervisórios estão cada vez mais presentes nos sistemas de automação, pois eles, além de oferecer ferramentas para um controle bastante efetivo do processo em si, como acionamentos e monitoramento de variáveis, permite ao pessoal do PCP (Planejamento e Controle de Produção) analisar tudo aquilo que está sendo produzido, sendo assim capaz de gerenciar melhor a compra com fornecedores, fornecimento a clientes, acompanhamentos estatísticos e etc.

Considerando o sistema de controle de acesso em ambiente industrial, todas estas funcionalidades serão aplicadas, mas no contexto deste trabalho. Analisando a situação, julga-se que seja importante para os gerentes analisar os **horários de entrada** e a **quantidade de acessos por dia**.

Para armazenar estes dados, foi escolhido o banco de dados SQL Server, que é gerenciado através da ferramenta SQL Management Studio. Nas tabelas do SQL, será possível realizar 3 ações referentes aos usuários: Adicionar, Editar e Remover.

2.1 SQL SERVER

Foi escolhida esta ferramenta para armazenamento dos dados de informações dos usuários e de horários de acesso. Para viabilizar seu funcionamento correto, foi feito o download do software através do site da Microsoft, bem como da sua ferramenta gerencial, o SQL Management Studio.

No SQL, foi criada a tabela Dados_Usuário, que contém as seguintes informações:

- **Senha (Chave Primária):** Esta é a coluna principal, e, diferente de muitos outros bancos de dados, a senha é a chave primária. Foi definido assim devido ao formato da interface de acesso da porta principal, onde terá uma IHM com apenas os botões para o usuário digitar sua senha sem necessidade de escrever o nome previamente. Ao digitar a senha, ela automaticamente já identifica o usuário que acessou o sistema. É usado como chave primária pois, em função da interface de acesso, não é possível existirem senhas iguais.

- **Nome:** Coluna de identificação do nome do usuário. Funcionará principalmente para elementos de pesquisa para informação de dados estatísticos.
- **Função:** Esta coluna indica a função daquele usuário no sistema, indicando se é aluno ou professor. Importante para as análises estatísticas.

A ferramenta Elipse Scada proporciona uma comunicação direta com este banco de dados, para tornar isto possível é necessária a criação de um ODBC (Open Database Connectivity). Mais a frente será explicado com mais detalhes este processo. Após esta etapa, cria-se uma conexão na ferramenta Organizer do Elipse Scada com a tabela Dados_Usuário criada, e isto automaticamente faz com que cada coluna da tabela vire uma tag.

Os tags são todas as variáveis (numéricas ou alfanuméricas) envolvidas no aplicativo. Os atributos são dados fornecidos pelo Elipse SCADA sobre parâmetros de sistema e componentes da aplicação. Como exemplo, podemos considerar uma tag a temperatura de um forno. Um de seus atributos poderia ser o nível de alarme a partir do qual deva ser acionada uma sirene [6].

2.2 COMUNICAÇÃO MODBUS

Para esta aplicação foi selecionado o protocolo de comunicação Modbus, o qual será abordado com mais detalhes adiante neste trabalho.

Para qualquer equipamento de Automação Industrial comunicar-se com o Sistema Supervisório, é necessário algum Driver de comunicação. Diversos fabricantes possuem diferentes Drivers, o que muitas vezes dificulta o trabalho, principalmente dos responsáveis pela manutenção, uma vez que o projeto necessite de um reparo que precise trocar o equipamento. Para sanar este problema, foram criadas as Redes Industriais, e neste caso, mesmo que haja uma troca de

equipamento, se ambos o anterior e o novo derem suporte à comunicação Modbus, a substituição é muito mais simples.

Para configurar a comunicação Modbus com o Elipse Scada, primeiro configura-se a leitura da .dll do Driver de comunicação, e em seguida configura-se as tags para acessarem o equipamento e o elemento desejado do PLC (Saída, Memória, Registrador e etc.).

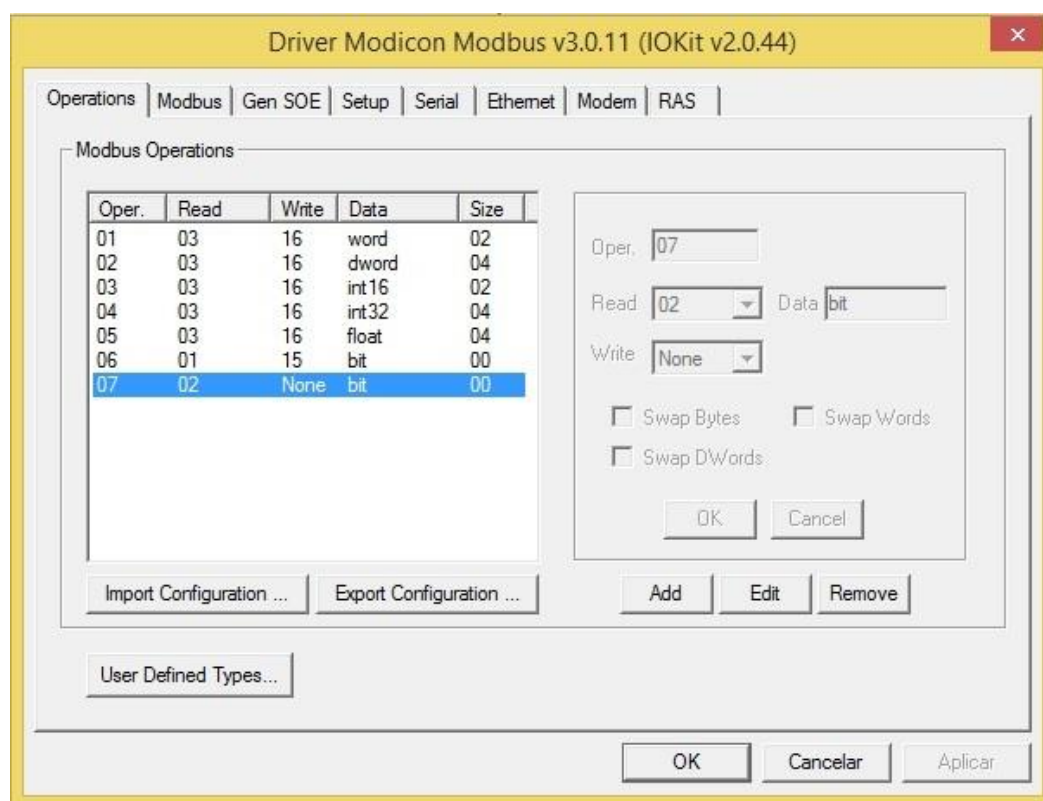


FIGURA 1 CONFIGURAÇÃO DO DRIVER DE COMUNICAÇÃO MODBUS

A imagem acima mostra a tela de configuração do Driver. Modbus Operations são as operações que podem ser realizadas pelo software. Cada operação é configurada para ler ou escrever em uma diferente região de memória. O Driver já vem com estas 7 operações diferentes de fábrica, mas é possível adicionar, editar ou remover cada uma.

Uma vez configurado o Driver para a comunicação, é necessário configurar a tag que irá ter acesso ao CLP. Para isto, será necessário apenas editar 4 parâmetros: N1, N2, N3 E N4

N1: Endereço do equipamento escravo na rede. Este endereço é usado em redes seriais e pode variar de 1 a 247. Pode-se ainda configurar este parâmetro com o valor 0 (zero). Com isto, este tag trabalha em modo **Broadcast**, enviando a mensagem para todos os equipamentos escravos (CLP) que estiverem na rede [6].

N2: Código da operação. Referencia uma das operações citadas na página anterior. É em geral modificado em função do tamanho do dado a ser lido.

N3: Parâmetro Adicional. Em geral não é usado e pode ser deixado em 0 (zero). [6]

N4: Endereço do registrador, variável ou bit do dispositivo que se deseja ler. Funciona como *offset*, pois o valor retornado será o valor do Endereço Base + N4 (Offset).

2.3 CADASTRO E SENHAS

Este projeto tem como principal funcionalidade o cadastro, adição e remoção de usuários através do sistema supervisor, dados os quais serão copiados no *CLP* para que haja uma independência do primeiro no caso de queda de servidor. Para um usuário poder ser adicionado, ele deverá ter uma senha única, e é esta que o identificará no momento de acesso. Visando este fato, foi necessária ser elaborada uma **política de construção de senhas**. As regras são:

- 1) Caracteres Iguais:** Nenhuma senha pode ter todos os caracteres iguais, isto facilitaria até para outros verem o usuário digitando sua senha no laboratório e decorar para poder usar a mesma. Para realizar esta verificação, foi dividida a *string* da senha em 2, através do código:

```
STR1 = Left(ID_Add,2)
STR2 = Right(ID_Add,2)
STR11 = Left(STR1,1)
STR12 = Right(STR1,1)
STR21 = Left(STR2,1)
STR22 = Right(STR2,1)
```

Onde a função Left (Variável, n) dá como resultado os n-ésimos números mais a esquerda, e a função Right (Variável, n) dá como resultado os n-ésimos números mais a direita.

Após esta divisão, temos todos os números da senha separados em diferentes variáveis. Através da função abaixo é possível saber o que se deseja:

```
STR1 == STR2 AND STR11 == STR12
```

Em palavras, isto significa que se os 2 primeiros dígitos forem iguais aos 2 últimos e o primeiro dígito igual ao segundo, a senha contém todos os caracteres iguais.

2) Números Crescentes ou Decrescentes: Esta regra implica que se uma senha tiver os caracteres em sequência numérica de ordem 1, ela é inválida. A sequência não pode ser nem crescente nem decrescente.

```
IF Len(ID_Add) == 4 Real(STR22) == (1+Real(STR21)) AND  
Real(STR21) == (1+Real(STR12)) AND Real(STR12) ==  
(1+Real(STR11))
```

Acima está a condição para testar se a senha é crescente, e abaixo a condição para testar se é decrescente.

```
IF Len(ID_Add) == 4 Len(ID_Add) == 4 AND Real(STR22) ==  
(Real(STR21)-1) AND Real(STR21) == (Real(STR12)-1) AND  
Real(STR12) == (Real(STR11)-1)
```

3) Senha Existente: Neste caso, não é possível que haja duas senhas iguais, pois o usuário é identificado pela sua senha no momento do acesso. O próprio banco de dados *SQL Server* não permite que se adicione outra senha igual, pois a coluna referente à senha é do tipo chave primária. Foi usada um algoritmo apenas para identificar se já existe senha igual e informar no momento da adição.

```

Dados_Usuário.Locate("ID == ID_Add", 1)
IF ID == ID_Add
MessageBox("Já contém um registro")
ERRO = 1
ENDIF

```

A função *Locate* realiza uma busca no banco de dados e, caso exista, armazenará a senha em ID, que será comparada com ID_Add, que é a senha digitada, e informada através de *MessageBox*.

2.4 REMOÇÃO

Da mesma forma que pode ser adicionado um usuário, é necessário que seja possível removê-lo também. Para isto, foi criada uma tela onde se pode procurar um usuário pelo nome, confirmar e em seguida remover.



FIGURA 2 TELA DE REMOÇÃO DE USUÁRIOS

O campo de pesquisa está atrelado à tag *Procura*, onde será armazenado o nome digitado. Para procurar este item na tabela, utiliza-se a função:

```

Dados_Usuário.Locate("Nome == Procura", 1)

```

O primeiro parâmetro da função *Locate* equivale à condição buscada, e o segundo indica que a busca iniciará do primeiro elemento da tabela. Caso o segundo elemento fosse 0, iniciaria da posição atual. Após encontrado, a remoção é feita através da função:

```
Dados_Usuário.DeleteRecord()
```

2.5 EDIÇÃO

Esta opção permite que se edite os dados do usuário. Propositalmente, foi escolhido para não se editar a coluna RG, pois é através dela que a tabela de estatísticas se baseia. Caso o usuário tenha escrito seu RG de forma incorreta inicialmente, o coordenador deve removê-lo do banco de dados e depois adicionar novamente da forma correta.

Edição

Edição de Usuário

	Atual	Novo
Nome	Alberto	0
Senha	2553	0
Função	Aluno	0
RG	4444444	0

Digite o RG

0

Alterar Nome

Alterar Senha

Alterar Função

Voltar

PROCURAR

de Usuários: 4

FIGURA 3 EDIÇÃO DE DADOS DOS USUÁRIOS

3 MODBUS

O protocolo Modbus foi desenvolvido inicialmente pela Modicon em 1979, sendo hoje um padrão aberto, mantido pela Organização Modbus¹, tendo sido implementado por centenas de fabricantes em milhares de equipamentos. A Schneider Electric, atual controladora da Modicon, transferiu os direitos do protocolo para a Organização Modbus em abril de 2004, firmando o compromisso de manter o protocolo aberto. A especificação pode ser obtida gratuitamente no site da Organização, e a utilização do protocolo é livre de taxas de licenciamento.

Por ser um protocolo aberto, desde o início teve fácil penetração no mercado e continua sendo bem-aceito, por sua simplicidade e certa robustez na troca de dados entre os dispositivos [5]. Originalmente, o protocolo foi implementado para comunicação RS-485, mas como é apenas uma estrutura de troca de mensagens, pode ser implementado em diversas camadas físicas. Três versões são as mais comuns: Modbus Plus, Modbus Serial e Modbus TCP/IP.

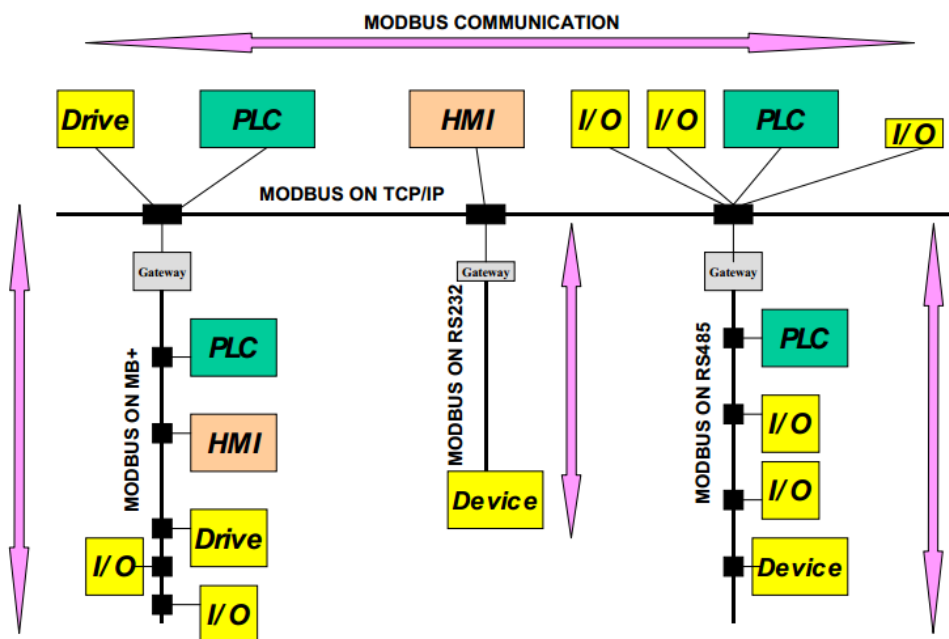


FIGURA 4 ARQUITETURA DE UMA REDE MODBUS

¹ www.modbus.org

3.1 MODBUS SERIAL

Normalmente utilizado para comunicação dos CLPs com blocos de E/S (*Entrada e Saída*) e com os instrumentos eletrônicos inteligentes, como relés de proteção, controladores de processo, atuadores de válvulas, transdutores de energia e outros. O meio físico utilizado é o RS-232 ou RS-485. A primeira permite a comunicação de apenas 2 dispositivos, e uma limitação de cabo de 20m. A segunda permite a comunicação de vários dispositivos numa mesma rede e cabos de comprimento de até 1200 metros. Os controladores podem ser configurados para comunicar-se em redes Modbus usando 2 modos de transmissão: Modbus RTU (*Remote Terminal Unit*) ou Modbus ASCII (*American Standart Code for Information Interchange*). Estes modos determinam como a informação será armazenada nos campos da mensagem.

- **Modbus ASCII:** No modo de comunicação ASCII, cada byte da mensagem é enviado em forma de 2 caracteres ASCII. A grande vantagem desse modo é que permite intervalos de até 1 segundo entre caracteres sem causar erro [7] (*Modicon Modbus)

Neste modo, as mensagens começam com o caractere “:” e terminam com o CRLF (Carriage Return – Line Feed). Os dispositivos presentes na rede continuamente estão monitorando o canal de comunicação em busca do caractere “:”, que indica início de comunicação.

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	<i>n</i> CHARS	2 CHARS	2 CHARS CRLF

FIGURA 5 FRAME DE MENSAGEM ASCII

- **Modbus RTU:** Neste modo de comunicação Serial, cada byte de mensagem é dividido em 2 caracteres hexadecimais de 4 bits cada. A grande vantagem do Modbus RTU é que sua densidade de caracteres permite uma melhor taxa de transferência que o Modbus ASCII. As mensagens podem ser transmitidas de forma contínua.

No modo RTU, as mensagens começam com um intervalo de silêncio de pelo menos 3.5 vezes um caracter, e o primeiro campo em seguida transmitido é o endereço do dispositivo. Os dispositivos da rede monitoram continuamente o canal de comunicação, e quando o primeiro campo (endereço do dispositivo) é recebido, cada equipamento decodifica para identificar se é o seu endereço, mas só será válido se estiver passado pelo menos 3.5 caracter de intervalo entre a mensagem anterior e a atual.

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1-T2-T3-T4	8 BITS	8 BITS	$n \times 8$ BITS	16 BITS	T1-T2-T3-T4

FIGURA 6 FRAME DE MENSAGEM RTU

3.2 MODBUS PLUS

É uma versão melhorada do Modbus RTU em alguns pontos, possibilitando que CLPs que trabalhem em modo Modbus se comuniquem entre si durante a execução do processo. Também pode trabalhar com blocos de E/S e outros dispositivos como relés de proteção e controladores diversos. O meio físico é o serial RS-485 com taxas de transmissão de até 1 Mbps (Megabit por segundo).

O Modbus Plus é baseado no *Token Passing*, um método de acesso que só permite um dispositivo utilizar um meio de transmissão em um dado momento.

3.3 MODBUS TCP

A rede Modbus TCP (*Transmission Control Protocol*) consiste de diversos dispositivos conectados através de uma rede TCP/IP, com interações que seguem o modelo cliente-servidor. O cliente envia uma mensagem ao servidor que por sua vez responde ao cliente com os dados requisitados. Esta transação ocorre através do envio de frames Modbus TCP por uma conexão TCP estabelecida previamente entre o cliente e o servidor. Uma vez estabelecida a conexão, o seu controle e gerenciamento são feitos pelo protocolo TCP/IP e ocorre independente do protocolo

Modbus. Para esta comunicação é utilizada a porta 502, a qual é reservada para aplicações com protocolo Modbus.

Os frames do Modbus TCP consistem dos seguintes campos:

- **Transaction Identifier:** Identifica a ordem da transação daquela informação. Serve como identificação, uma vez que diversas mensagens atravessam o mesmo canal no mesmo período de tempo.
- **Protocol Identifier:** Utilizado para identificar o protocolo.
- **Length:** Identifica o tamanho da mensagem, em bytes.
- **Unit Identifier:** Usado para identificar o dispositivo que receberá a mensagem (escravo).

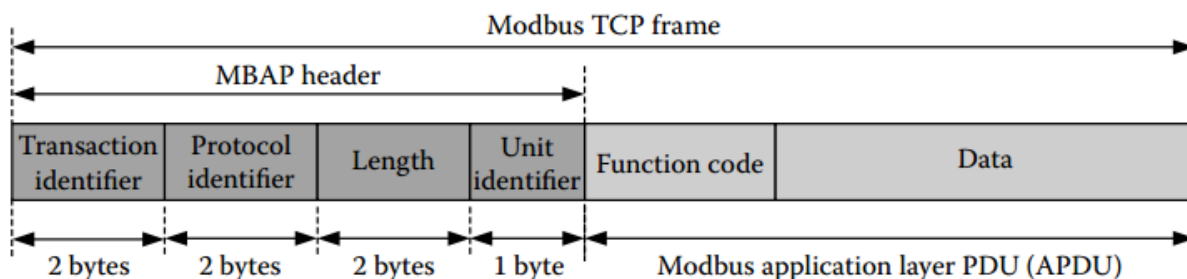


FIGURA 7 FRAME MODBUS TCP

Diferentemente do Modbus Serial, os frames do Modbus TCP não possuem campo de detecção de erro. Isto é desnecessário, uma vez que o próprio protocolo TCP/IP inclui diversos mecanismos de detecção de erro.

3.4 APLICAÇÃO

Para este trabalho, foi utilizado o protocolo Modbus RTU, que é o utilizado pelo Elipse Scada para se comunicar com o CLP TPW-03. Nesta aplicação, o mais importante é que seja escrito em uma lista de memórias do CLP todas as senhas que estão armazenadas no banco de dados SQL. Para isto, foi criado uma tag no supervisão denominada Registrador_Base_Senhas e outra denominada Flag_CLP. A primeira foi configurada para escrever no registrador D4 do CLP as senhas presentes no banco de dados uma a uma. Após escrita cada senha, escreve-se o valor 1 em Flag_CLP, que é o registrador D8 do controlador. Uma vez que o valor de

Flag_CLP volta para 0, o supervisor entende que deve escrever a próxima senha. O papel do CLP nesta operação é realocar cada senha escrita na posição correta de memória.

Abaixo segue o código escrito em Script do Elipse Scada que realiza este algoritmo:

```
Contador = 0
Dados_Usuário.MoveFirst()
WHILE Contador < Dados_Usuário.GetTotalNumberOfRecords()
  IF Flag_CLP.Read() == 0
    Registrador_Base_Senhas.WriteEx(ID)
    Contador += 1
    Flag_CLP.WriteEx(1)
    Dados_Usuário.MoveNext()
  ENDIF
WEND
```

The screenshot shows the 'Geral' (General) tab of a configuration window for a device named 'Registrador_Base_Senhas'. The window has four tabs: 'Geral', 'Alarmes', 'Scripts', and 'Referência-Cruzada'. The 'Geral' tab is active. It contains the following fields and controls:

- Nome:** A text box containing 'Registrador_Base_Senhas' and a button 'Mudar tipo para...'.
- Descrição:** A text box containing 'Registrador_Base_Senhas' and a button 'Acessar bits...'.
- Driver:** A dropdown menu showing 'Modbus - Driver Modicon Modbus v3.0.1' and a button 'Ajuda'.
- Parameters:** Five input boxes labeled N1, N2, N3, N4, and Scan, with values 1, 1, 0, 4, and 1000 respectively.
- Escala (Scale):** A section with a checkbox 'Escala' (unchecked). It contains four input boxes: 'CLP Inferior' (0), 'CLP Superior' (20000), 'Sist. Inferior' (0), and 'Sist. Superior' (20000).
- Testa conexão aqui (Test connection here):** A section with a 'Valor' (Value) input box (0) and two buttons 'Ler' (Read) and 'Escrever' (Write).
- Options:** Three checked checkboxes: 'Habilita leitura pelo scan' (Enable reading by scan), 'Habilita leitura automática' (Enable automatic reading), and 'Habilita escrita automática' (Enable automatic writing).

FIGURA 8 CONFIGURAÇÃO DE REGISTRADOR_BASE_SENHAS

Contador é a variável que auxiliará a percorrer todos os elementos da tabela. A função MoveFirst() faz com que inicie no primeiro elemento. Então, se Flag_CLP tiver o valor 0, significa que pode haver uma escrita, logo ele escreve em Registrador_Base_Senhas, soma 1 no contador e escreve 1 em Flag_CLP, para indicar que terminou a escrita. A tabela move para o próximo elemento e fica no aguardo de Flag_CLP voltar para o valor 0 para iniciar a nova escrita.

4 SQL SERVER

O SQL Server é um sistema gerenciador de banco de dados relacional de propriedade da *Microsoft*. Sua principal função é armazenar e recuperar os dados solicitados por outras aplicações, seja no mesmo computador ou em outros.

Embora o *software Elipse Scada* tenha a opção de poder armazenar seus dados em um arquivo de extensão .dat, o banco de dados SQL permite que estes dados possam ser armazenados em servidores, aumentando a segurança da informação.

Para a efetiva gestão da ferramenta *SQL Server*, foi necessário realizar a instalação do *software SQL Management Studio*, disponibilizado pela *Microsoft* na Internet. Para o funcionamento perfeito do *SQL Server* com a ferramenta *Elipse Scada*, foram necessários realizar os seguintes passos:

4.1 INSTALAÇÃO DO SQL SERVER

Software disponibilizado pela *Microsoft* no seu endereço eletrônico². O cuidado principal para realizar o *download* desta ferramenta é atentar-se para a arquitetura do processador (32 ou 64 bits). Sendo assim, foi necessário averiguar esta informação para baixar a versão correta deste *software*.

4.2 INSTALAÇÃO DO SQL MANAGEMENT STUDIO

Esta ferramenta também é disponibilizada pela *Microsoft* no mesmo website. O *Microsoft SQL Server Management Studio Express* é um ambiente de desenvolvimento integrado gratuito para acessar, configurar, gerenciar, administrar e desenvolver todos os componentes do SQL Server. Ele combina um amplo grupo de

² www.microsoft.com

ferramentas gráficas e editores de script sofisticados para fornecer acesso ao *SQL Server* a desenvolvedores e administradores de todos os níveis de conhecimento.

4.3 CRIAÇÃO DE TABELAS

Uma vez instaladas estas ferramentas, dá-se início à criação das tabelas que serão utilizadas para armazenamento das informações. Neste trabalho, foram criadas duas tabelas: *Dados_Usuário* e *Estatísticas*

4.3.1 Dados_Usuário

Esta tabela armazena os dados dos usuários cadastrados. Cada vez que alguém for inserido no sistema, haverá uma inserção nesta tabela. Igualmente uma remoção. Nela, temos 4 colunas:

- **ID:** Esta é a chave primária, onde é armazenada a senha do usuário. Foi escolhida como chave primária pois não pode haver senhas repetidas no sistema. Tipo: *Int*
- **Nome:** Nome completo do usuário. Tipo: *Varchar*
- **Função:** A função que ele desempenha no laboratório. Tipo: *Varchar*
- **RG:** Identificação do usuário. É utilizado principalmente para relacionar com a tabela *Estatísticas*, pois é através dela que se sabe as informações de acesso do usuário. Uma vez criado, o RG não pode ser alterado. Tipo: *Varchar*

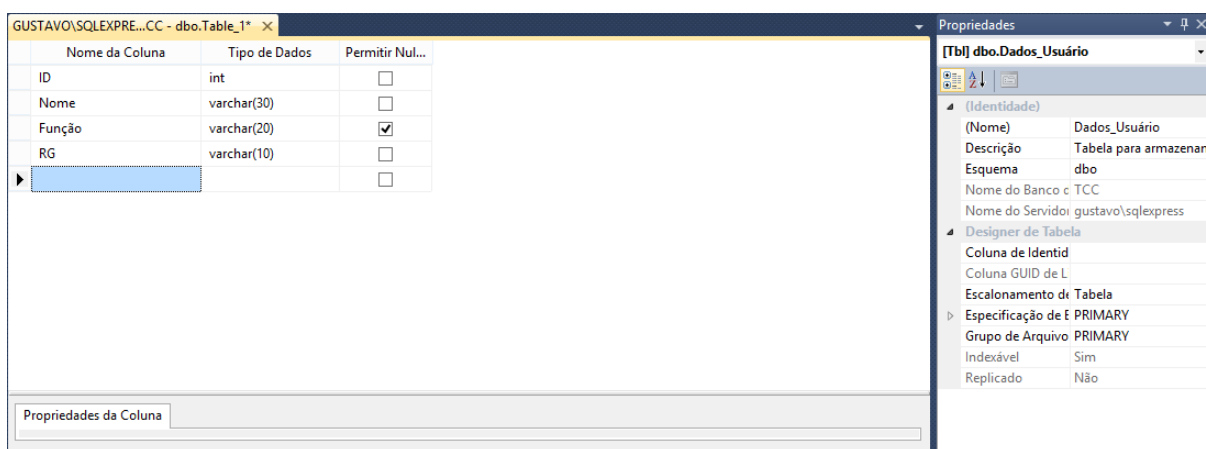


FIGURA 9 CRIAÇÃO DA TABELA *DADOS_USUÁRIO*

4.3.2 Estatísticas

Esta tabela armazena as informações de acesso dos usuários. Cada vez que um usuário acessa o sistema, é adicionado um elemento a esta tabela, com as informações RG e Data/Hora de acesso. A princípio havia-se pensado em criar uma tabela para cada usuário, onde esta tabela iria armazenar todas as informações de acesso, no entanto, a ferramenta *Elipse Scada* não tem a opção de criação nem remoção de tabelas, apenas manuseio das tabelas já existentes. Nesta tabela, temos 2 colunas:

- **RG:** Armazena o RG do usuário que acessou o laboratório em determinado momento. Esta coluna não pode ser de chave primária, pois existirão várias instâncias com o mesmo RG. Por exemplo, se um usuário acessou dia 10/07 às 14h e depois no mesmo dia às 16h, haverão dois elementos na tabela com o mesmo RG e horários diferentes. Tipo: Varchar
- **Data:** Armazena a data e a hora exatas de cada acesso do usuário. Tipo: Datetime

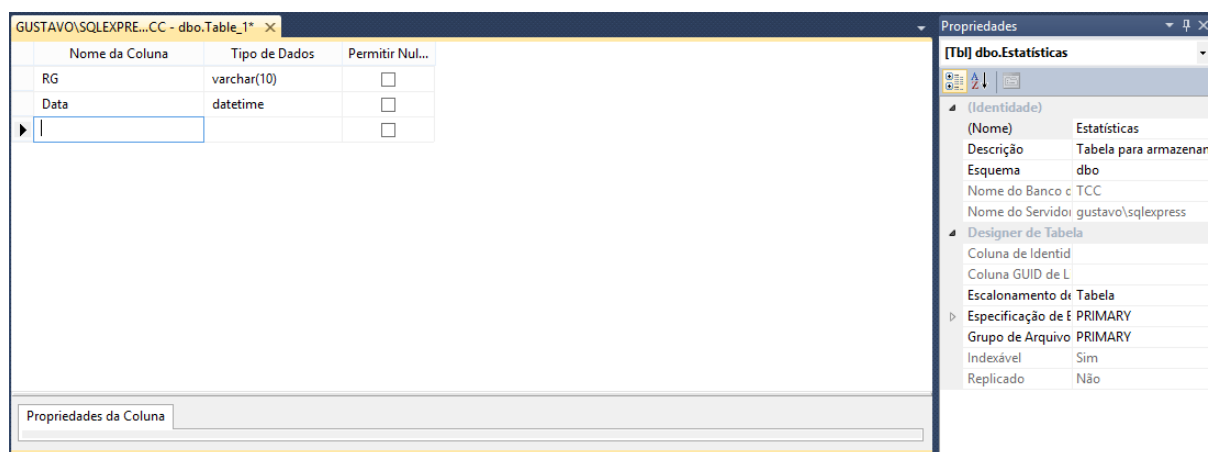


FIGURA 10 CRIAÇÃO DE TABELA ESTATÍSTICAS

4.5 ODBC

Open Database Connectivity (ODBC) é a interface estratégica da Microsoft para acessar dados em um ambiente heterogêneo de relacional e não-relacional sistemas de gerenciamento de banco de dados. Com base na especificação da Interface de nível de chamada do grupo de acesso SQL, ODBC fornece uma maneira de abrir, independente de fornecedor de acessar dados armazenados em uma variedade de proprietários de PC, minicomputador e bancos de dados de mainframe. ODBC diminui a necessidade de fornecedores independentes de software e desenvolvedores corporativos para aprender várias interfaces de programação de aplicativo. ODBC agora fornece uma interface de acesso a dados universal. Com ODBC, os desenvolvedores de aplicativos podem permitir que um aplicativo simultaneamente acessar, exibir e modificar dados de vários bancos de dados diferentes [8].

Foi necessária a criação de um ODBC para poder haver interface do *SQL Server* com a ferramenta *Elipse Scada* para ela poder ler as informações do banco de dados SQL.

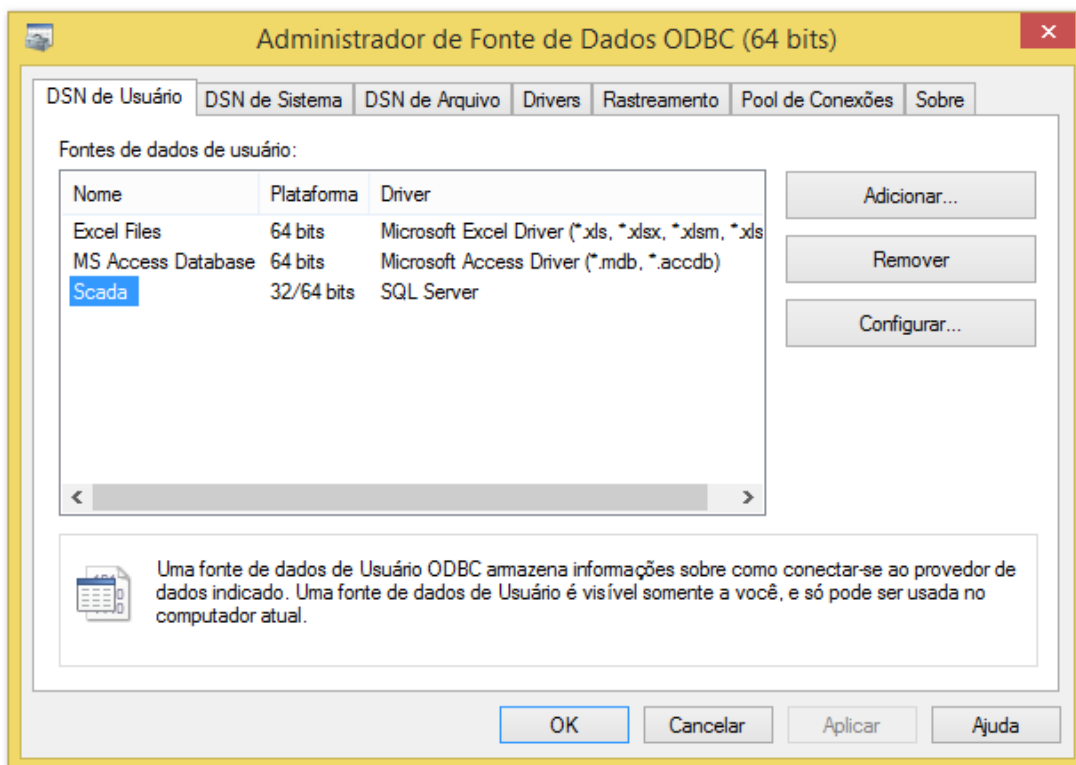


FIGURA 11 CRIAÇÃO DO ODBC SCADA

5 CONSIDERAÇÕES FINAIS

A princípio, a idéia deste projeto era pra funcionar todo baseado em CLP e IHM, no entanto, identificou-se essa necessidade de aprimoramento devido à questão de melhor tratamento de dados armazenados, o que só seria possível através de Sistemas Supervisórios e Bancos de Dados.

Um dos primeiros problemas desde trabalho foi a decisão de armazenar as informações de acesso toda no CLP, para, cada vez que o operador do Supervisório selecionasse a opção *Upload*, os dados fossem atualizado no banco de dados. Observamos que para isto, teria de ser necessário ocupar uma memória muito maior no CLP, e depois ter estar sujeito a um trabalho manual de selecionar a opção de atualizar. Optamos então por fazer isso de forma mais otimizada e automatizada: a cada acesso do usuário ao laboratório, era enviada a informação ao Supervisório e ele atualizava as estatísticas. Caso o computador com o *Elipse Scada* estivesse inativo, isso não seria um problema grande, pois estas informações não são críticas e podem ser descartadas por um curto período de tempo sem maiores problemas.

Outro desafio encontrado foi o armazenamento das senhas, que seria a princípio apenas em Bancos de Dados, no entanto, observou-se que essa era uma questão crítica, pois se o servidor estivesse fora do ar, ninguém conseguiria acessar o laboratório. Para isto, foi criada a opção de atualizar o CLP, a qual, cada vez que selecionada, transfere todas as senhas do Banco de Dados SQL para uma região de memória pré-definida no controlador.

Através deste trabalho, pudemos verificar como são importantes os equipamentos de Automação para oferecer um controle de acesso mais robusto e seguro para os ambientes industriais e para comprovar que as ferramentas utilizadas no ramo da Automação Industrial são bastante completas a ponto de realizar funções que muitas vezes não envolvem controle de máquinas e processos necessariamente.

REFERÊNCIAS

- [1] W. E. Santos e P. R. d. Silveira, Automação e Controle Discreto, Érica, 2009.
- [2] F. Prudente, Automação Industrial - Plc: Teoria e Aplicações - Curso Básico, LTC, 2011.
- [3] B. G. Wilamowski e J. D. Irwin, Industrial Communication Systems, LLC, 2011.
- [4] WEG, “WEG,” [Online]. Disponível em: <http://www.weg.net/br>. [Último acesso em 20 Julho 2015].
- [5] I. M. Parede e L. E. Gomes, Eletrônica Automação Industrial, Fundação Padre Anchieta, 2011. [Último acesso em 20 Julho 2015].
- [6] E. S. Ltda., “Eclipse,” 10 Dezembro 2008. [Online]. Disponível em: www.elipse.com.br. [Último acesso em 20 Julho 2015].
- [7] I. A. S. MODICON Inc., “Modbus,” Junho 1996. [Online]. Disponível em: <http://www.schneider-electric.com>. [Último acesso em 20 Julho 2015].
- [8] M. Corporation, “Microsoft,” Microsoft Corporation, 03 Março 2007. [Online]. Disponível em: www.microsoft.com.br. [Último acesso em 20 Julho 2015].