AMBIENTE DIDÁTICO PARA SIMULAÇÃO DE REDE INDUSTRIAL UTILIZANDO O PROTOCOLO MODBUS TCP/IP

Vitor Alexandre Santos – vitorsantoss@gmail.com
Universidade Tecnológica Federal do Paraná – UTFPR
Av. Sete de Setembro, 3165
CEP 80230-901 – Curitiba – Paraná

Ricardo Domingues Soares – ricardo.soares@pr.senai.br
Serviço Nacional de Aprendizagem Industrial (Paraná) – SENAI
Rua Senador Accioly Filho, 298
CEP 81.310-000 – Curitiba – Paraná

Resumo: *Este trabalho consiste na implementação de uma ferramenta para simulação de rede industrial com foco no protocolo Modbus TCP/IP. Esse simulador é desenvolvido e testado com o software Excel da Empresa Microsoft Corporation, não onerando custos, já que os computadores utilizados já possuem o mesmo instalado. Assim, por meio de alguns equipamentos, como exemplo o CLP (Controlador Lógico Programável), disponível em laboratórios de automação, são testados envios e recebimentos de dados por meio do protocolo citado, com o simulador implementado. A utilização de uma ferramenta de baixo custo, ou até mesmo inexistente, como é o caso da aplicação em questão, permite o auxílio de atividades práticas em disciplinas de redes industriais, as quais muitas vezes são tratadas somente no formato teórico, devido à indisponibilidade de equipamentos em laboratório. Inicialmente o artigo apresenta o protocolo Modbus TCP/IP e descreve o desenvolvimento do simulador. Na sequência apresenta as redes implementadas com os testes em torno do protocolo e finaliza com a exposição dos resultados obtidos assim com sugestões para novos trabalhos.*

Palavras-chave: *Simulador, Redes industriais, Modbus TCP/IP, Controlador lógico programável.*

1. INTRODUÇÃO

Crescentes demandas de trocas de informações dentro de um processo industrial, elevada complexidade de dados, segurança humana em máquinas, entre outros assuntos relacionados com o tema de redes industriais, evidenciam a importância do mesmo em setores automatizados em ambientes fabris (MORAES & CASTRUCCI, 2007). Dessa forma, estudos pertinentes ao campo das redes de comunicações em torno de processos de sistemas de manufatura ou sistemas contínuos de automação, se mostram com elevada aceitação entre profissionais e estudantes da área citada.

Relacionado o exposto com a área de ensino, Queiroz et al (2010) afirma que

atividades práticas auxiliam no processo de aprendizado, podendo ser apoiadas por ferramentas de simulação. Carvalho et al (2010) salienta a importância de ferramentas que auxiliem em atividades práticas, seja para propósito didático ou para testes em torno de aplicações existentes.

Tomando como ponto de partida o uso de simuladores, relacionado com o tema de redes industriais, diversos trabalhos pesquisados apresentam tal prática, demonstrando a relevância de tais ferramentas no ensino em cursos relacionados à automação. Como exemplo, Mossin (2007) apresenta em seu trabalho um laboratório para ensino de controle de sistemas distribuídos via rede de campo com o protocolo *Foundation Fieldbus*. Complementando o trabalho de Mossin, Martins (2013) apresenta um laboratório para testes de automação de processos com acesso remoto, via rede de comunicação, assim como Casini et al (2003), que também desenvolve simuladores de sistemas dinâmicos via acesso remoto.

Dessa forma, com o objetivo no auxilio de atividades práticas em disciplinas relacionadas a redes industriais, esse trabalho apresenta um simulador para testes em redes *Modbus TCP/IP*. Esse simulador é implementado sem a necessidade de investimentos financeiros em equipamentos, permitindo somente, com o uso do *software* Excel, acessar dados na rede, seja para envio ou recebimento de informações.

De maneira resumida, inicialmente o artigo faz uma introdução sobre o protocolo *Modbus TCP/IP*, para que, na sequência sejam tratadas questões do desenvolvimento do simulador. Em seguida apresenta os testes aplicados, assim como os resultados obtidos. Nas conclusões são apresentadas sugestões para trabalhos futuros.

2. O PROTOCOLO MODBUS TCP/IP

O protocolo *Modbus* foi desenvolvido pela Modicon na década de 1970. É um protocolo aberto e amplamente difundido no setor industrial, utilizado por diversos fabricantes relacionados ao meio de automação de sistemas. O *Modbus* é um protocolo da camada de aplicação para troca de dados entre dispositivos de controle (SCHNEIDER, 2016).

O *Modbus* pode ser implementado em diversos padrões e meios físicos, como exemplo o RS232, RS422, RS485 (padrões seriais) e o *Ethernet*. Dessa forma, conforme o padrão utilizado, o protocolo difere quanto ao número de dispositivos conectados, distância entre os mesmos, velocidades nas transmissões de dados, entre outros.

Considerando as redes seriais, o *Modbus* pode ser do tipo RTU (*Remote Terminal Unit*) ou ASCII (*American Standart Code for Information Interchange*), os quais diferem entre si pelo formato do telegrama de transferência e como ele é tratado. Para o padrão *Ethernet* tem-se o *Modbus TCP/IP*, que é o quadro *Modbus* sobre a pilha *Ethernet TCP/IP*. Dessa forma é possível uma taxa de transferência mais elevada em distâncias maiores que as permitidas pelos padrões seriais.

O protocolo *Modbus TCP/IP* possui como tecnologia de comunicação, o conceito de cliente e servidor, onde o cliente tem o domínio do tráfego de dados na rede e os servidores atendem as requisições geradas pelos clientes, de forma análoga ao conceito mestre e escravo no padrão RS485 para o *Modbus RTU*. Quanto ao algoritmo de acesso ao meio, por ser um protocolo executado sobre o padrão *Ethernet*, aplica o CSMA-CD (*Carrier Sense Multiple Access with Collision Detection*).

Sobre a pilha TCP/IP, o *Modbus TCP/IP* adiciona um quadro específico denominado MBAP (*Modbus Application Protocol*), tendo como modelo uma mensagem composta pelo MBAP (sete *bytes*), código da função e dado de transferência.

Considerando o padrão *Ethernet*, o dispositivo na rede *Modbus TCP/IP* necessita do endereçamento IP (*Internet Protocol*) assim como a porta TCP, a qual depende do serviço na camada de aplicação. Como serviços comuns estão o FTP (*File Transfer Protocol*), o HTTP (*Hypertext Transfer Protocol*), DNS (*Domain Name System*), entre outros. Para a comunicação em questão, para a porta *Modbus*, tem-se como padrão o valor 502.

Para a troca de dados sobre o protocolo, são dispostas as funções *Modbus*, as quais definem se a comunicação será de escrita ou leitura de dados, por exemplo. Entre as funções mais aplicadas, têm-se as mostradas na Tabela 1.

Tabela 1 - Principais funções *Modbus*.

Código da Função	Descrição
1	Leitura de dado do tipo *coils* (saída discreta)
2	Leitura de bits do tipo entrada discreta
3	Leitura de bloco de registradores do tipo *holding*
4	Leitura de bloco de registradores do tipo entrada
5	Escrita de dado do tipo *coils* (saída discreta)
6	Escrita de dado em registrador tipo *holding*

A partir da função *Modbus*, tem-se os endereços das áreas de registros que são lidos ou escritos. Esses endereços são padronizados segundos o protocolo. A Tabela 2 mostra os endereços utilizados para o referido protocolo.

Tabela 2 - Endereços dos registros *Modbus*.

Endereço	Tamanho	Descrição
00001 - 09999	1 *bit*	*Coils* (Leitura e escrita)
10001 - 19999	1 *bit*	Entradas discretas (Somente leitura)
30001 - 39999	16 *bits*	Registros de entrada (Somente leitura)
40001 - 49999	16 *bits*	Registros tipo *holding* (Leitura e escrita)

3. DESENVOLVIMENTO DO SIMULADOR

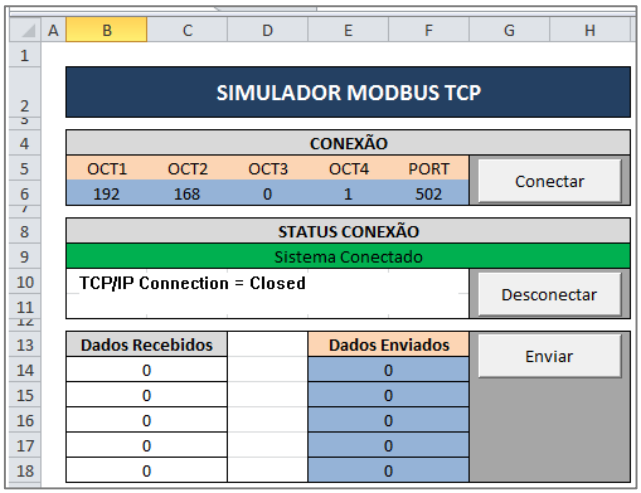
Para o desenvolvimento do simulador é utilizado o *software Excel* da Empresa *Microsoft Corporation*. Na elaboração da planilha, que representa o simulador, é utilizado um controle *Activex*, o qual é disponibilizado pela *Witte Software*. Um controle *Activex* é um pequeno programa denominado complemento, o qual, para a aplicação do simulador, é adicionado pelo VBA (*Visual Basic for Applications*) do *Excel*. O *Activex* utilizado é intitulado como MBAX e é utilizado no formato de demonstração, assim ele disponibiliza condições para comunicação com o protocolo *Modbus* a partir da planilha implementada.

O controle *Activex* de demonstração tem por característica a manutenção da comunicação por sessenta minutos, desconectando os dispositivos servidores após esse tempo. Para a aplicação em questão, essa característica é irrelevante, pois em situações de simulação em aulas de redes industriais, caso a rede caia, é necessário somente

conectá-la novamente, já que nenhum dispositivo está em campo realizando uma aplicação, por exemplo.

Com o controle *Activex* adicionado, é elaborada uma planilha, a qual funciona como cliente em uma rede *Modbus TCP/IP*. Na planilha são disponibilizados campos para inserir o endereço IP do servidor da rede, por meio dos quatro octetos assim como a porta TCP necessária. Um campo de verificação de *status* da rede também é implementado para monitoração da conexão, assim como campos de leitura de informações da rede e escrita de dados no servidor conectado. A Figura 1 mostra a planilha utilizada como simulador de cliente *Modbus TCP/IP*.

Figura 1 - Planilha utilizada como cliente *Modbus TCP/IP*.



São configurados três botões na planilha, para conexão e desconexão com o servidor e envio de dados. Esses botões executam códigos escritos em VBA a partir de bibliotecas disponibilizadas com o controle *Activex* MBAX adicionado.

Para a conexão do servidor na rede é tomado como base código mostrado na Figura 2, o qual foi retirado da documentação do controle *Activex.*

Figura 2 - Código para conexão do cliente com o servidor *Modbus TCP/IP*.

Examples Use TCP/IP

```
MBAXP1.Connection = 0
MBAXP1.TCPIPPort = 502
MBAXP1.IPAddr1 = 235
MBAXP1.IPAddr2 = 12
MBAXP1.IPAddr3 = 134
MBAXP1.IPAddr4 = 6
MBAXP1.Timeout = 1000
MBAXP1.OpenConnection()
If MBAXP1.GetLastError <> 0 Then
   MsgBox "Open connection error"
End If
```

No código utilizado são retiradas as constantes utilizadas nos octetos do endereço IP e da porta TCP, sendo inseridas referências às células da planilha, para flexibilizar a conexão com servidores diferentes.

Para envio e recebimento de dados são tomados como base os códigos da Figura 3 e Figura 4. Esses códigos também são retirados da documentação do *Activex*. Para o código de envio são utilizados os registradores do protocolo *Modbus,* o endereço do dispositivo na rede, o comprimento do dado e o tempo para a conexão.

Figura 3 - Código para envio de dados via *Modbus TCP/IP*.

```
Preset 4 holding registers starting from address 40003 in slave ID 9. Read every 1000ms

Dim e As Integer

Private Sub Command1_Click()
  e = Mbaxp1.PresetMultipleRegisters(1, 9, 2, 4, 1000)
  Mbaxp1.Register(1, 0) = 1
  Mbaxp1.Register(1, 1) = 2
  Mbaxp1.Register(1, 2) = 4
  Mbaxp1.Register(1, 3) = 8
  Mbaxp1.UpdateEnable (1) 'Start continuously update
End Sub
```

No código de recebimento de dados, os parâmetros configurados são semelhantes aos de envio, utilizando também a área de registro da *Modbus*, endereço do dispositivo, comprimento do dado e tempo de conexão.

Figura 4 - Código para recebimento de dados via *Modbus TCP/IP*.

```
Read 10 holding registers starting from address 40005 from slave ID 3. Read every 700ms

Dim e As Integer

Private Sub Command1_Click()
  e = Mbaxp1.ReadHoldingRegisters(1, 3, 4, 10, 700)
  Mbaxp1.UpdateEnable (1) 'Start continuously update
End Sub
```

No desenvolvimento da planilha, os códigos são adaptados para a aplicação em questão. Os códigos mostrados nas Figuras 3 e 4 são apenas referência para o desenvolvimento das funções necessárias da planilha. Os códigos reais não são mostrados em detalhes devido à extensão do assunto. Na sequência são tratadas as redes implementadas, assim como os testes aplicados.

4. APLICAÇÕES EM REDE COM CLP

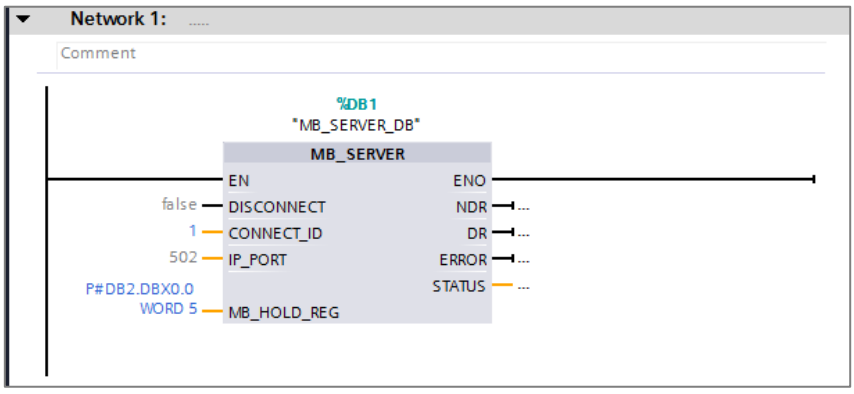
O simulador desenvolvido é configurado como cliente em uma rede *Modbus TCP/IP*. Com isso, para os testes aplicados, são utilizados controladores lógicos programáveis configurados como servidores de rede para o protocolo em questão. Para resultados mais abrangentes em torno do simulador, dois modelos de controladores são utilizados, de duas marcas diferentes. É utilizado o S7-1200 CPU 1214C da Empresa *Siemens* e o TM221 da Empresa *Schneider Electric*, os quais são mostrados na Figura 5.

Figura 5 - Controladores utilizados: (a) S71200 CPU 1214C da *Siemens*; (b) TM221 da *Schneider Electric*

4.1. S7-1200 CPU 1214C - *Siemens*

Para os testes com o CLP S7-1200, é utilizado o *software* TIA (*Totally Integrated Automation*) Portal na versão 13. A linguagem de programação é a *ladder* conforme IEC61131-3. Dessa forma é desenvolvido um programa para troca de cinco dados do tamanho de *word* (16 *bits*). Segundo a especificação do protocolo *Modbus*, os dados trocados são referentes aos registros do tipo *holding*, endereçados nas áreas 40001 a 49999, para leitura e escrita de valores. A Figura 6 mostra o bloco utilizado no programa do CLP, o qual utiliza os dados com cinco *word*, assim como a porta TCP/IP.

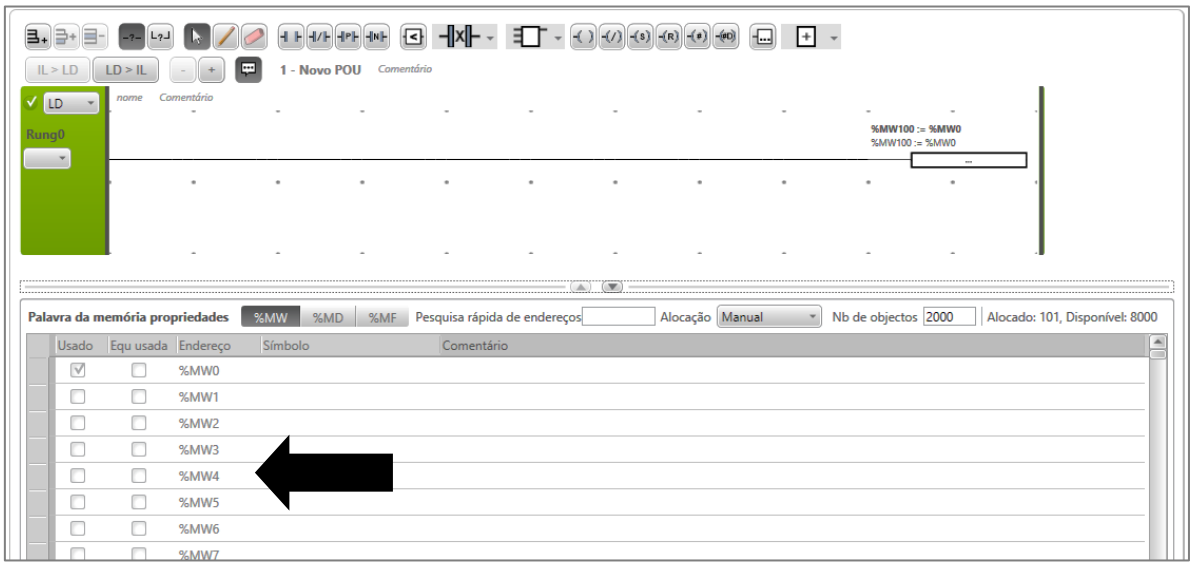
Figura 6 - Bloco de programa do CLP S7-1200



4.2. TM221 - *Schneider Electric*

Para os testes com o TM221, é utilizado o *software SoMachine Basic* na versão 1.4. Esse CLP executa a função de servidor da rede *Modbus TCP/IP*, sendo necessário somente atribuir um endereço IP para o mesmo. A partir dessa configuração, as áreas de memórias disponíveis para utilização na programação, já recebem os dados da rede. Dessa forma, as memórias, mostradas na Figura 7, recebem os valores dos registros da rede, referentes às áreas, de 40001 a 49999, e essas podem ser utilizadas no decorrer do programa. Para o projeto em questão, elas são somente recebidas e enviadas para comprovação da funcionalidade do simulador.

Figura 7 - Área de memória do CLP TM221



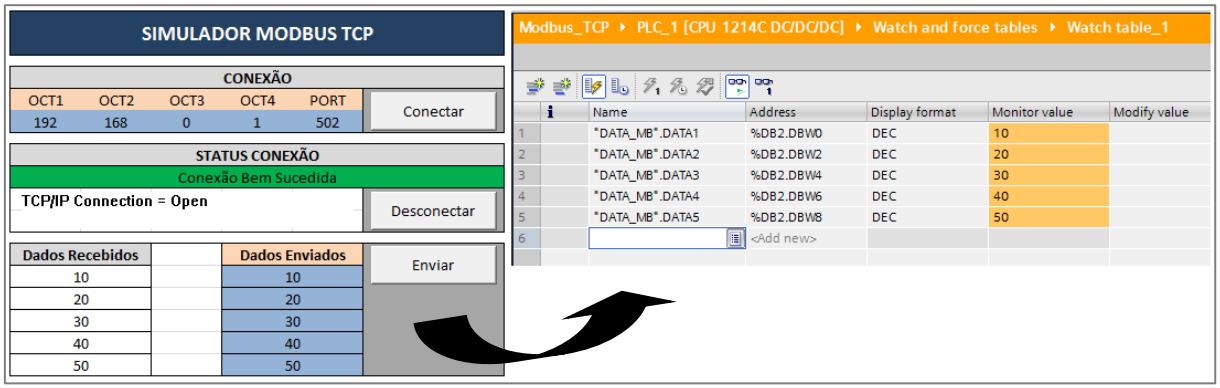
5. ANÁLISE DOS RESULTADOS

Para análise dos resultados, os controladores, são conectados ao simulador de forma individual. Primeiramente é testado o CLP S7-1200 da *Siemens* e na sequência o CLP TM221 da *Schneider*.

O simulador (cliente) é configurado com o endereço IP do CLP (servidor), assim como a porta TCP/IP 502, padrão para conexão da rede *Modbus TCP/IP*. Na sequência são enviados conjuntos de dados, os quais são compostos por cinco variáveis com comprimento de *word*. A Figura 8 mostra a troca de dados entre o simulador e o CLP S7-1200. Para o primeiro caso, são enviados pelo simulador, os seguintes valores: 10, 20, 30, 40 e 50, sendo um para cada *word*, definida na comunicação. É possível verificar ao lado da tabela do simulador, a interface do CLP no modo *online*. Assim, ao enviar os dados, são monitorados os mesmos valores.

Como a área de recebimento de dados do simulador é a mesma de envio, registros 40001, 40002, 40003, 40004 e 40005, é possível verificar os mesmos valores enviados. Importante salientar que esses dados recebidos pelo simulador são do CLP, e não os próprios dados enviados.

Figura 8 - Troca de dados entre o simulador e o CLP S7-1200 da *Siemens*



De forma análoga a comunicação anterior, é realizada a troca de dados do simulador com o CLP TM221 da *Schneider*.

Na Figura 9, é possível verificar o envio de um conjunto de dados pelo simulador e o recebimento do CLP. O conjunto de dados é formado pelos valores 100, 200, 300, 400 e 500. Ainda na Figura 9, é possível verificar ao lado do simulador a monitoração *online* do CLP. Como no teste anterior, a área de recebimento de dados do simulador ainda é mesma de envio, registros 40001, 40002, 40003, 40004 e 40005, assim é possível verificar os mesmos valores enviados. Da mesma forma, também é importante salientar que os dados recebidos pelo simulador são do CLP, e não os próprios dados enviados.

Figura 9 - Troca de dados entre o simulador e o CLP TM221 da *Schneider*

6. CONSIDERAÇÕES FINAIS

Esse trabalho apresenta um simulador de dispositivo cliente em uma rede industrial *Modbus TCP/IP*. Com isso, é possível a troca de dados com qualquer equipamento que possua o protocolo *Modbus TCP/IP* incorporado, e assim possa se comportar como um servidor para o protocolo de rede em questão.

Para os testes executados, somente CLPs são utilizados, no entanto, qualquer dispositivo pode ser aplicado em conjunto com o simulador, como exemplo, inversores de frequência, conversores de sinais, interfaces homem máquina, entre outros, desde que disponibilizem tal interface de comunicação.

Dessa forma, além de auxiliar em laboratórios de ensino, como o proposto por esse artigo, este simulador pode ser aplicado na rotina de trabalho de desenvolvedores de soluções baseadas em automação, já que muitas vezes os equipamentos não estão disponíveis, ou a infraestrutura do cabeamento não está finalizada.

Considerando a aplicação em bancadas didáticas, este simulador permite, de maneira simplificada, testes e estudos sobre o protocolo *Modbus TCP/IP*, pois somente com um cabo de rede ligado no computador e no dispositivo em estudo (servidor), já é possível a execução de tarefas referente à troca de dados.

Como trabalhos futuros, pode ser desenvolvido um simulador para o mesmo protocolo, ou seja, o *Modbus*, porém para o padrão serial, como: RS232, RS485 ou RS422, considerando o *Modbus RTU* e o *ASCII.*

No geral, conclui-se que o trabalho cumpriu os requisitos para simulação de cliente *Modbus TCP/IP*, podendo ser aplicado desde atividades práticas em cursos de redes industriais, assim como ferramenta de apoio de profissionais da área de automação industrial.

REFERÊNCIAS BIBLIOGRÁFICAS

CARVALHO, R. T., BALDIOTI, H. R., SILVA, N. L., GOMES, F. J. Módulo Laboratorial para Educação em Controle, em Tempo Real, Baseado em Linux/RTAI. Anais: XVIII - Congresso Brasileiro de Automatica. Bonito, 2010.

CASINI, M.; PRATTICHIZZO, D.: VICINO, A. E-learning by remote laboratories: a new tool for control education. In: IFAC Symposium On Advances In Control Education. Oulu, 2003.

MARTINS, Luis Miguel Silva; INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA, Departamental de Engenharia Mecânica. Projecto dum Laboratório Remoto para Automação de Processos Industriais, 2013. 91p, il. Dissertação (Mestrado).

MORAES, C.C. de; CASTRUCCI, P. L. Engenharia de Automação. 2.ed. LTC, 2007.

MOSSIN, Eduardo André; UNIVERSIDADE DE SÃO PAULO, Escola de Engenharia de São Carlos. Laboratório Remoto para Ensino de Sistemas de Controle Distribuídos, 2007. 168p, il. Dissertação (Mestrado).

QUEIROZ, F. P., FREITAS, L. P., GAWA, V. A., GOMES, F. J. Desenvolvimento de uma Plataforma HILS para Educação em Controle de Processos Baseada em FOSS. Anais: XVIII - Congresso Brasileiro de Automática. Bonito, 2010.

ORGANIZAÇÃO MODBUS. **Citação de referências e documentos eletrônicos.** Disponível em: <http://www.modbus.org/> Acesso em: 16 abr. 2017.

SCHNEIDER. **Citação de referências e documentos eletrônicos.** Disponível em: <http://download.schneider-electric.com/files?p_Reference=DIA3ED2160105EN&p_EnDocType=Catalog&p_File_Id=1836802826&p_File_Name=DIA3ED2160105EN.pdf> Acesso: 24 mai. 2017.

SIEMENS. **Citação de referências e documentos eletrônicos.** Disponível em: <https://support.industry.siemens.com/cs/mdm/107623221?c=73837491339&pnid=13683&lc=en-WW> Acesso: 24 mai. 2017.

DIDACTIC ENVIRONMENT FOR INDUSTRIAL NETWORK SIMULATION USING THE PROTOCOL MODBUS TCP/IP

Abstract: *This work is the implementation of a simulator for industrial network with the Modbus TCP/IP protocol. This simulator is developed and tested in laboratories UTFPR with Excel software of Company Microsoft Corporation, not generating costs because computers used have already installed. Thus, by means of PLC (Programmable Logic Controller), available in the laboratory automation, data exchanges are tested using the protocol and simulator implemented. The use of a low cost tool, or non-existent, as in the case of the application allows the aid of practical activities in industrial networks subjects , which are often treated in theory only, due to unavailability of laboratory equipment. Initially the article presents the Modbus TCP/IP protocol and describes the development of the simulator. Following shows the networks implemented with the testing protocol and ends with the display of the results and suggestions for further work.*

Key-words: *Simulator, Industrial networks, Modbus TCP/IP, Programmable logic controller.*