INSTITUTO FEDERAL DO ESPÍRITO SANTO - CAMPUS SERRA
ENGENHARIA DE CONTROLE E AUTOMAÇÃO

GABRIEL SAADE PAGANI
RENAN GEORGIO CARVALHO CUZZUOL

SISTEMA INTEGRADO DE SUPERVISÃO UTILIZANDO REDE MODBUS

SERRA
2019
INSTITUTO FEDERAL DO ESPÍRITO SANTO - CAMPUS SERRA

ENGENHARIA DE CONTROLE E AUTOMAÇÃO

GABRIEL SAADE PAGANI

RENAN GEORGIO CARVALHO CUZZUOL

SISTEMA INTEGRADO DE SUPERVISÃO UTILIZANDO REDE MODBUS

Relatório apresentado à disciplina de Redes Industriais do curso de Engenharia de Controle e Automação do Instituto Federal do Espírito Santo, como avaliação parcial para aprovação na referida disciplina. Orientado pelo Professor Dr. Rafael Emerick.

SERRA

2019

SUMÁRIO

1. OBJETIVOS

Este trabalho tem como objetivo desenvolver sistema de monitoramento remoto utilizando protocolo de comunicação MODBUS. O sistema é composto por um PLC Rockwell Micrologix 1100, um sistema supervisório em IHM Rockwell PanelView Plus 400, e um dispositivo multimedidor EasyLogic PM1200 da Schneider – capaz de medir uma grande variedade de grandezas elétricas como corrente, tensão, fase, frequência, potência, potência aparente, fator de potência etc.

2. DESCRIÇÃO DO SISTEMA

2.1. Arquitetura do sistema

Uma escolha inicial importante foi definir qual seria o protocolo de comunicação entre os dispositivos do sistema. A comunicação escolhida entre o PLC e a IHM foi Ethernet (TCP/IP), devido à alta taxa de transmissão (entre 10 Mbps e100 Mbps devido à limitação das interfaces de rede do PLC e da IHM que não suportam o GigaEthernet) e a facilidade de configuração nesses dispositivos. Já para a transferência de dados entre o multimedidor e o PLC, foi escolhido o protocolo MODBUS. A Figura 1 a seguir mostra a arquitetura de rede do sistema proposto:

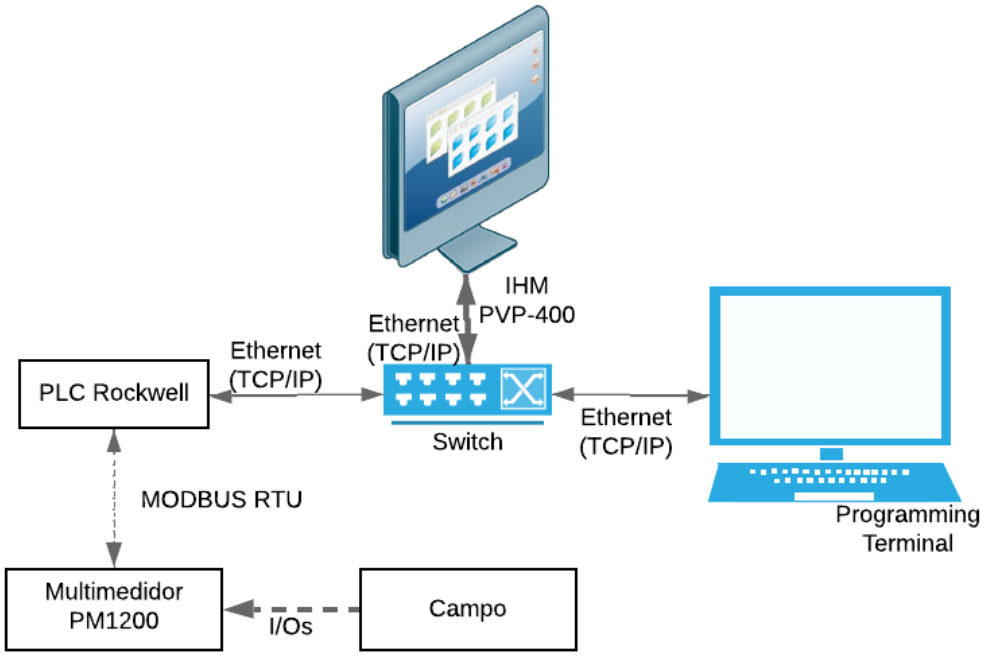

Figura 1: Arquitetura do sistema

A rede Ethernet configurada foi a 192.168.1.0, com máscara 255.255.255.0.

2.2. Descrição dos componentes e interfaces de comunicação

2.2.1. Sistema de Controle

O controlador utilizado foi o PLC Rockwell Micrologix 1100. O software de programação utilizado é o RSLogix 500, e a linguagem de programação escolhida foi o LADDER.

A CPU possui interface Ethernet padrão, mas para a comunicação com o Multimedidor, foi necessário instalar um módulo MODBUS NC-01.

Para acessarmos o PLC através do Terminal de Programação via Ethernet, é necessário primeiro configurar um IP na CPU, uma vez que a mesma vem de fábrica sem nenhum IP configurado. Para isso, é utilizado o *software* BOOTP/DHCP Server conforme Figura 2. Esse *software* envia pacotes broadcast na rede e aguarda resposta dos dispositivos conectados nela. Uma vez que recebe uma resposta, o endereço MAC do dispositivo é mostrado em uma lista, e então é possível atribuir um endereço de IP ao dispositivo com esse MAC, conforme Figura 3.

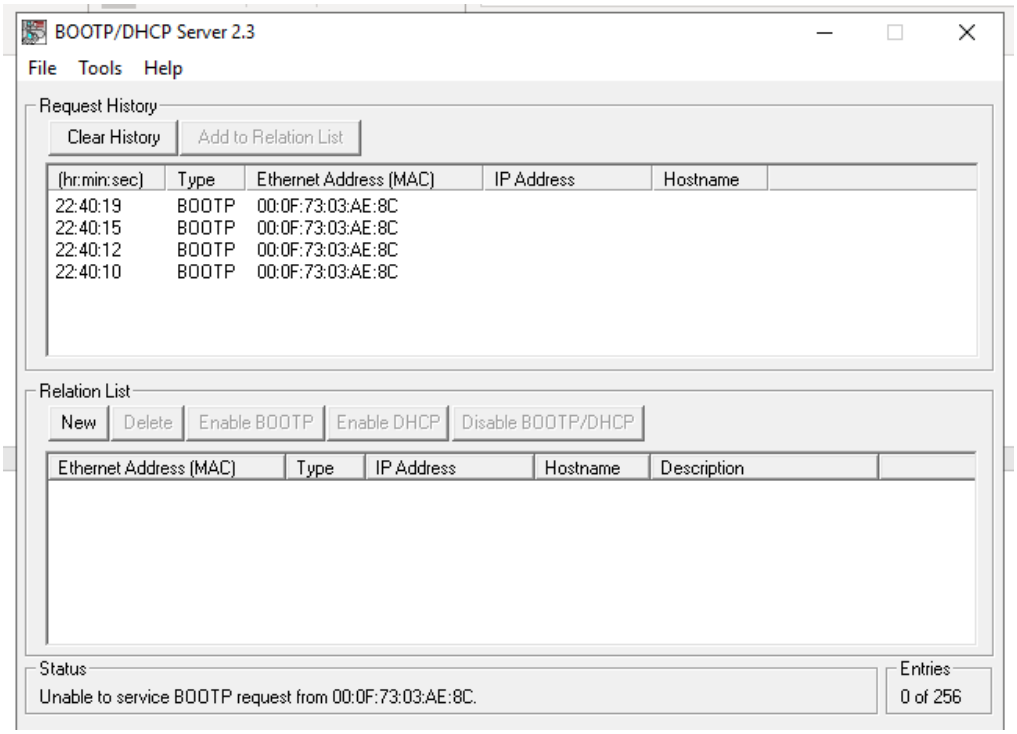

Figura 2: BOOTP/DHCP Server recebendo respostas de dispositivos na rede

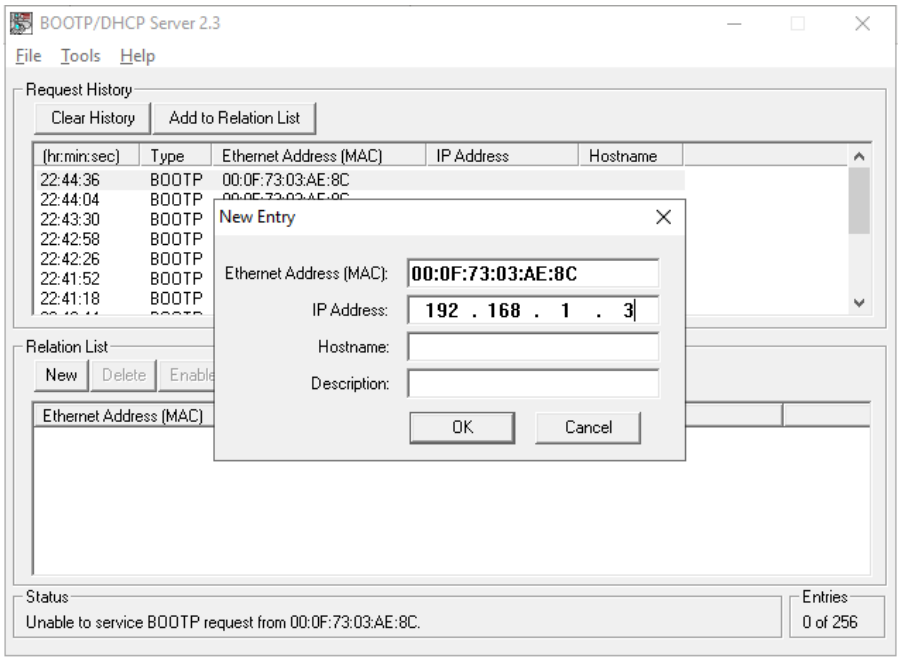

Figura 3: BOOTP/DHCP Server - Atribuindo Endereço de IP ao dispositivo

Após a configuração do endereço IP ao dispositivo, é possível descarregar o programa na CPU.

As configurações dos canais de comunicação foram feitas conforme Figuras 4 e 5.

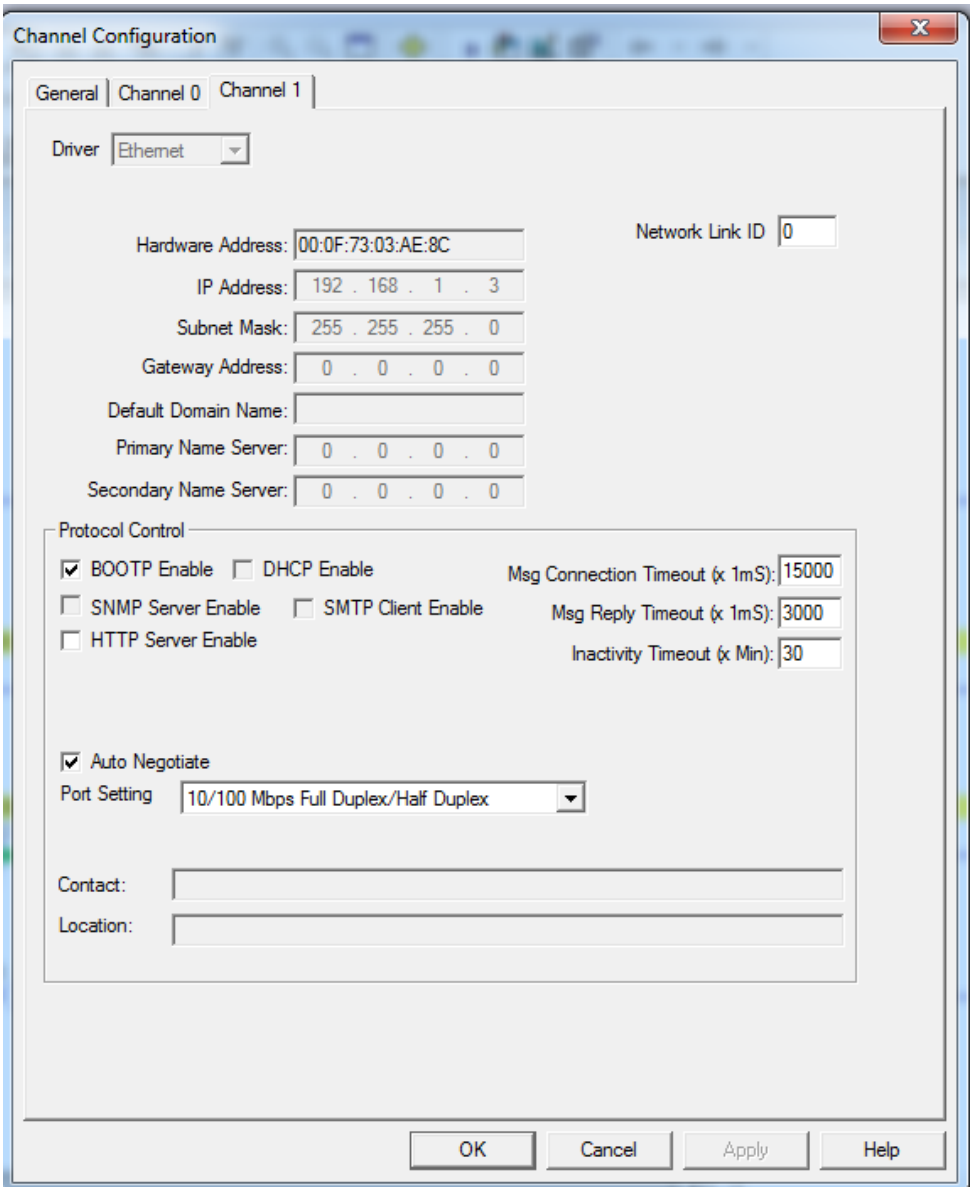

Figura 4: Configuração da porta Ethernet do PLC

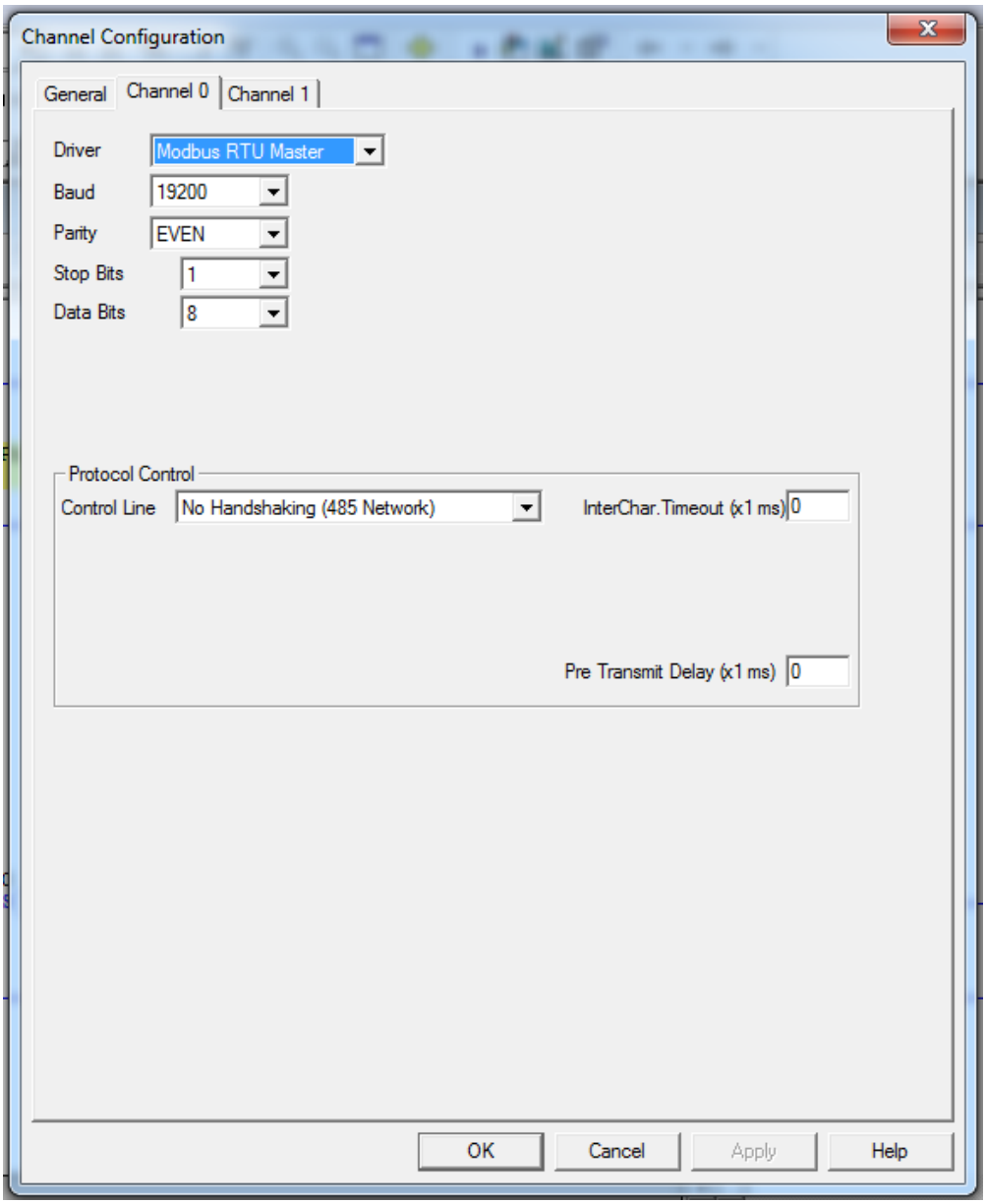

Figura 5: Configuração da interface MODBUS

O envio e recebimento de dados via MODBUS se dá através de blocos MSG, conforme Figura 6. Na tela de configuração do bloco, é definido o Comando MODBUS a ser usado nessa instância do bloco (Figura 7), o endereço dos dados no mestre, a quantidade de registradores envolvidos nessa instância, o tamanho do dado enviado/recebido, o tempo de time-out da mensagem, o endereço dos dados no escravo e o endereço do escravo.

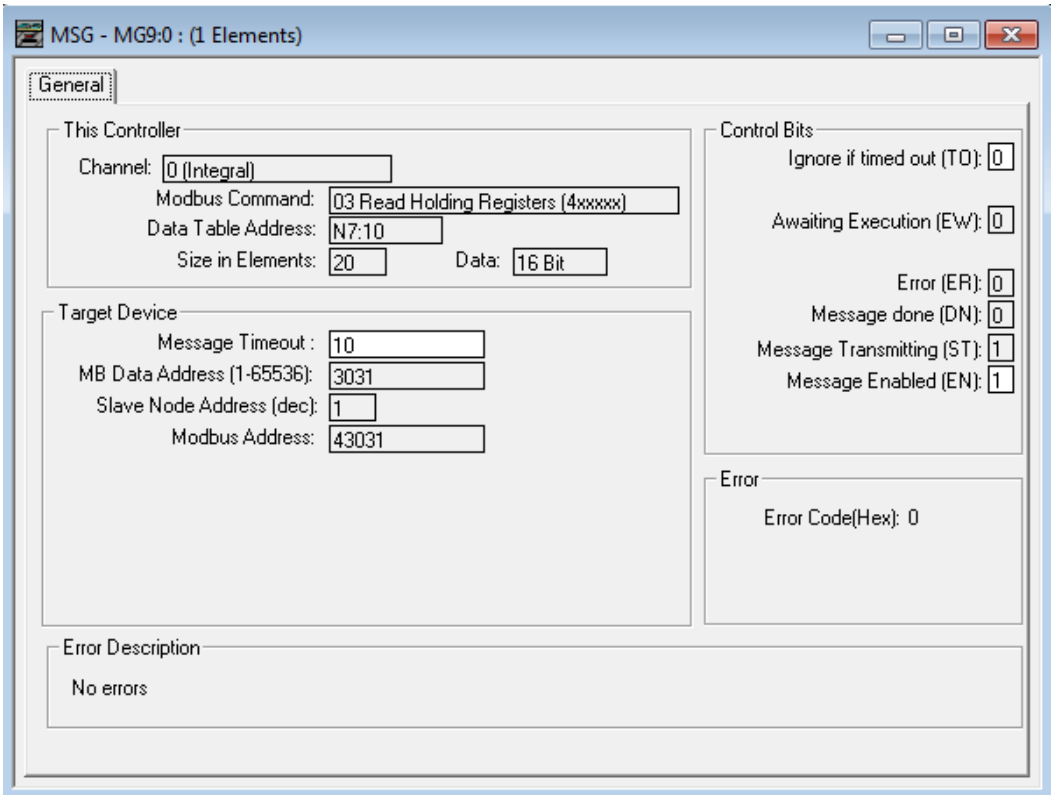

Figura 6:Exemplo de configuração do bloco MSG para comunicação MODBUS

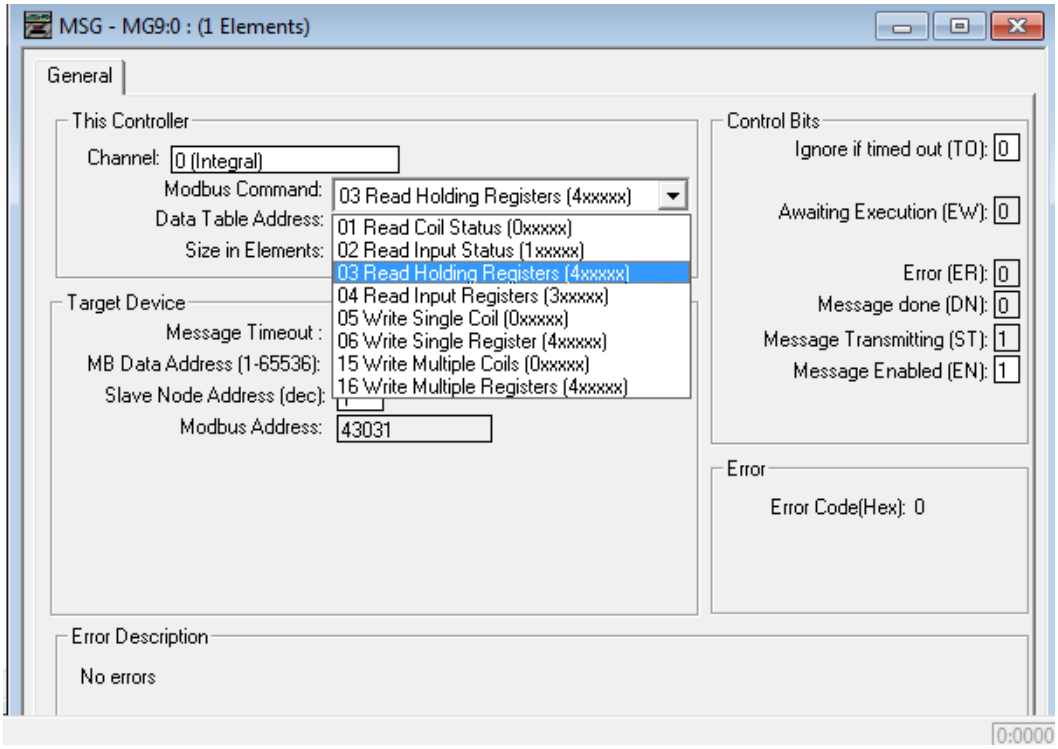

Figura 7: Exemplo de configuração do bloco MSG para comunicação MODBUS - Comandos MODBUS

A Figura 8 mostra o trecho do LADDER onde está implementada a leitura dos dados da Fase R do multimedidor, através do bloco MSG configurado conforme Figura 6.

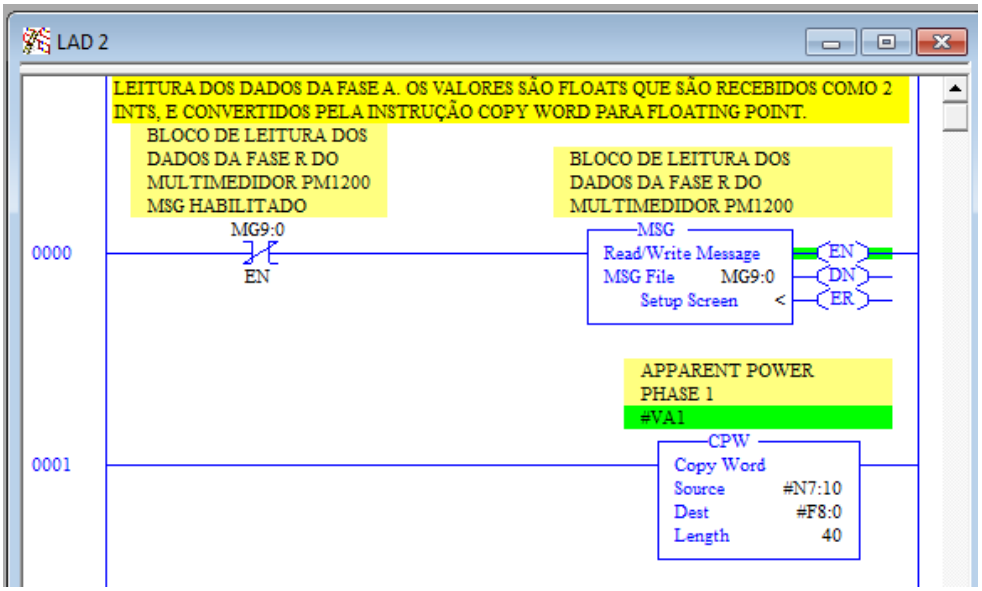

Figura 8: Código LADDER de leitura via MODBUS de dados do MP1200

2.2.2. Dispositivo de campo – Instrumento inteligente

O dispositivo escolhido foi um multimedidor EasyLogic modelo PM1200 da Schneider Electric. Trata-se de um instrumento capaz de medir simultaneamente tensões e correntes trifásicas, calcular potência real, aparente, entre diversos outros dados relevantes à sistemas elétricos em geral. Possui interface RS-485 com suporte ao protocolo MODBUS. O mapeamento de memória para comunicação MODBUS é encontrada em seu manual, e a Figura 9 mostra um trecho do capítulo de “Comunicações” dele.

R phase RMS Block:

- Function Code: 03H Read
- No of Registers: 20
- No Scaling Required
- Read as Block only

Table 6-6: R phase RMS block

Parameter	Description	Address	Type	PM1200
VA1	Apparent power, phase1	3031	Float	•
W1	Active power, phase1	3033	Float	•
VAR1	Reactive power, phase1	3035	Float	•
PF1	Power factor, phase1	3037	Float	•
V12	Voltage phase1 to phase2	3039	Float	•
V1	Voltage phase1 to neutral	3041	Float	•
A1	Current, phase1	3043	Float	•
F1	Frequency, Hz	3045	Float	•
Reserved	Reserved	3047	Long	
Intr1	Number of interruption	3049	Long	•

Figura 9: Trecho do manual do multimedidor PM1200 - Mapeamento de memória para comunicação MODBUS

Os dados do tipo Float ocupam dois registradores, portanto são transmitidos como 2 inteiros. No PLC é necessário fazer a “tradução” destes inteiros para Float novamente após o recebimento.

Os parâmetros de configuração do multimedidor são descritos na figura 10. É possível ler e escrever nesses registradores através da rede MODBUS, alterando assim os parâmetros do dispositivo.

SETUP Block:

- Function Code: 03H Read, 10H Write
- No of Registers: 40
- No Scaling Required
- Read and write as block only

Table 6-18: SETUP block

Parameter	Description	Address	Type	Range	Default value	PM1200
A.Pri	Current Primary	0101	Float	1.0 to 99 k	100.0	•
A.Sec	Current Secondary	0103	Float	1.0 to 6.5	5.000	•
V.Pri	Voltage Primary	0105	Float	100.0 to 999 k	415.0	•
V.Sec	Voltage Secondary	0107	Float	50.00 to 601.0	415.0	•
SYS	System Configuration	0109	Float	2.0 to 6.0 2.0 – Delta 3.0 – Star 4.0 – Wye 5.0 – 2 Ph 6.0 – 1 Ph	3.000	•
LABL	Phase Labeling	0111	Float	0.0 to 4.0 0.0 – 123 1.0 – ABC 2.0 – RST 3.0 – PQR 4.0 – RYB	0.000	•
VA Fn	VA Function selection	0113	Float	0.0 to 1.0 0.0 – 3D 1.0 – Arth	0.000	•
D sel	Demand Selection	0115	Float	0.0 to 1.0 0.0 – Auto 1.0 – User	0.000	•
D Par	Demand parameter	0117	Float	0.0 to 2.0 0.0 – VA 1.0 – W 2.0 A	0.000	•

Figura 10: Trecho do Bloco de endereços de Setup do MP1200

Antes de integrar o dispositivo na rede, é necessário configurar os parâmetros da comunicação serial através do display de navegação do mesmo. É necessário consultar o manual para identificar os possíveis valores para a configuração da comunicação, e é essencial configurar o dispositivo de acordo com a rede pré-configurada no Mestre, caso contrário a troca de dados não será possível.

2.2.3. Sistema de Supervisão

O sistema supervisório proposto consiste em uma IHM Rockwell modelo PanelView Plus 400, rodando o *software* de supervisão FactoryTalk Machine Edition. O *software* de programação da IHM é o FactoryTalk View Studio. A IHM possui interface Ethernet padrão, não sendo necessário o uso de nenhum tipo de adaptador ou conversor. A configuração do endereço de IP é feita diretamente no dispositivo, através do visor e teclado. O endereço separado para a IHM foi o 192.168.1.2.

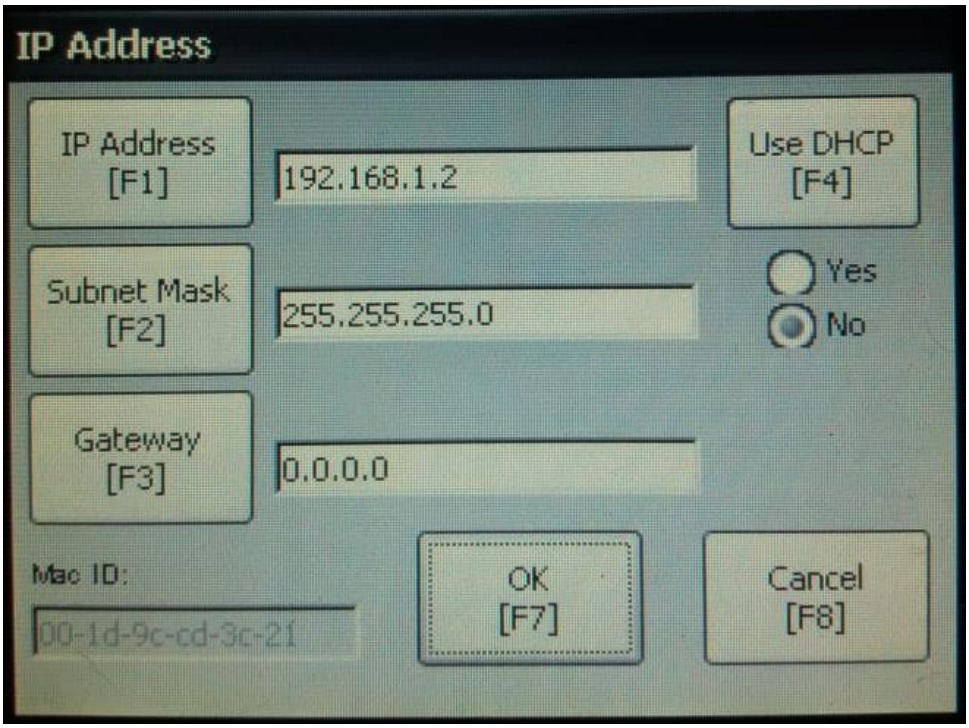

Figura 11: Configuração da interface Ethernet da IHM

Para a comunicação entre o PLC e a IHM, é necessário configurar o driver de comunicação *FactoryTalk Lynx*, dentro do *FactoryTalk View Studio*. Nele, configuramos um "atalho" (*shortcut*), e associamos a ele o PLC e seu endereço de IP, conforme Figura 12.

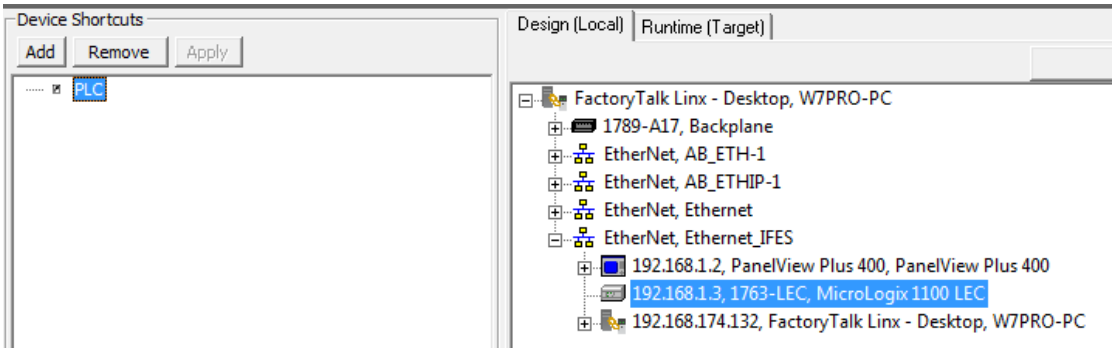

Figura 12: Configuração do driver de comunicação FactoryTalk Lynx

Com o driver configurado, é possível acessar na IHM dados do PLC diretamente através do "*shortcut* + endereço do dado no PLC", sem a necessidade de criar um novo endereço na IHM para ele.

2.3. Sistema integrado de supervisão

A figura 13 mostra a tela do supervisório desenvolvida para análise dos dados do multimedidor.

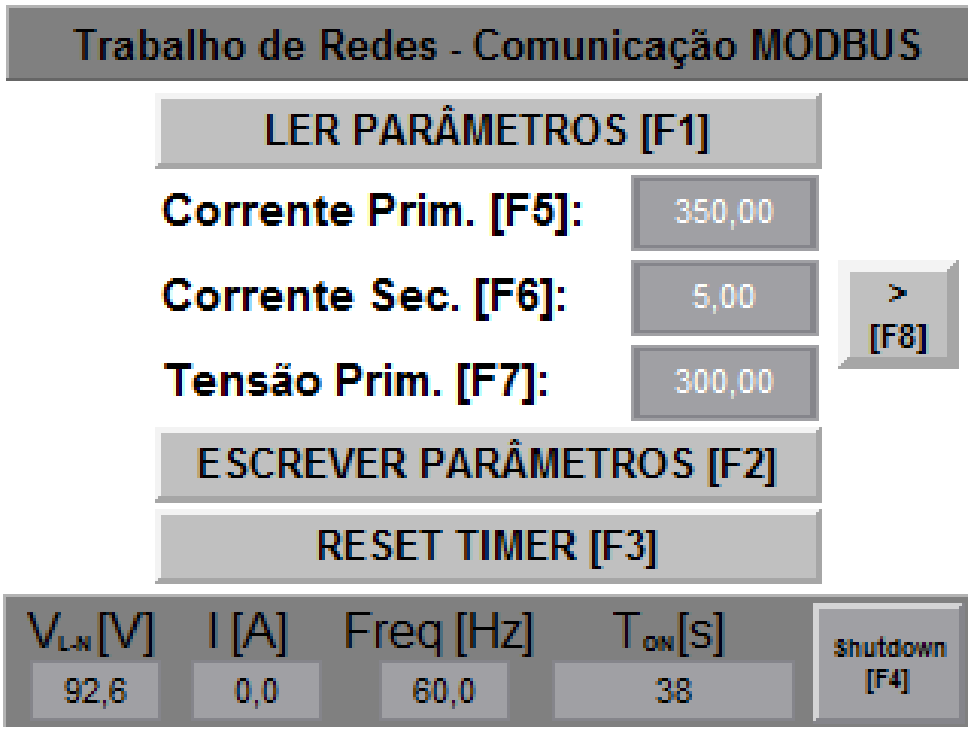

Figura 13: Tela de supervisão

Os botões F1 e F2, quando pressionados, habilitam a execução do bloco MSG responsável por ler e escrever, respectivamente, os dados dos parâmetros de configuração do PM1200. O botão F8 é usado para navegar entre os parâmetros. Para editar algum dos campos, basta navegar até a tela que contém o campo desejado, e pressionar o botão correspondente. Após a edição na IHM, é necessário enviar os dados para o PM1200 através do botão F2 – Escrever parâmetros.

Os dados de Tensão, Corrente, Frequência e Tempo Funcionando são atualizados constantemente, não sendo necessários comandos do operador. É possível enviar um comando de "Reset" do temporizador através da tecla F3.

3. RISCOS ENVOLVIDOS E SEGURANÇA

O sistema proposto é implementado em rede TCP/IP local, cabeada, sem uso de gateways ou roteadores e usando somente IPs não roteáveis. Dessa forma, para ter acesso aos dados dessa rede, é preciso uma conexão física direta à uma porta do Switch através de um cabo de rede. Portanto, não é necessária a implementação de nenhum tipo de criptografia ou qualquer outro método de segurança de dados em software, uma vez que o controle de acesso ao meio físico é possível e eficaz para garantir a segurança dos dados. Porém, caso não seja possível garantir o controle de acesso ao meio físico da rede, a rede estaria completamente vulnerável à ataques.

4. LINK PARA O REPOSITÓRIO GITHUB

Os códigos estão disponíveis em https://github.com/gabrielspagani/SistIntSupervisao.