TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

Gateway industrial ACL para Modbus TCP

Aristóteles R*, Leão TF*

**Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, IFSP, São Paulo, Brasil.*

Resumo. A maioria dos processos industriais possui computadores responsáveis por gerenciar as etapas da produção, são as *workstations*. Elas monitoram e controlam equipamentos (Inversores de frequência, parafusadeira e outros) através do envio de comandos via rede. Esse artigo expõe um sistema de comunicação entre um manipulador robótico e uma *workstation*, ambos detentores dos protocolos Modbus TCP e *Advanced Control Language* (ACL), respectivamente. Os dispositivos mencionados não se comunicam de forma direta, pois os protocolos de comunicação são diferentes. Sendo assim, não é possível realizar essa integração entre os equipamentos, ocasionando a falta de operação de um setor da planta industrial. Existem diversos problemas similares a esse em sistemas de automação, por isso há a utilização do *gateway* em diversos processos, visto que ele é uma tecnologia empregada na conversão entre protocolos, sendo assim o objeto de estudo desse artigo. A metodologia inicia na configuração do *gateway* de acordo com os parâmetros da *workstation* e o manipulador robótico, e posteriormente empregar o uso do monitorador de rede Wireshark a fim de verificar se os dados enviados e recebidos seguem as especificações solicitadas.

Palavras-chave. *ACL, integração, Gateway, Modbus TCP*

Abstract. *Most industrial processes have computers responsible for managing the production stages, which are the workstations. They monitor and control equipment (frequency inverters, screwdrivers and others) by sending commands via the network. This article shows a communication system between a robotic manipulator and a workstation, Modbus TCP and Advanced Control Language (ACL) protocols, respectively. The devices mentioned do not communicate directly, as the communication protocols are different. Therefore, it is not possible to perform this integration between the equipment, causing a sector of the industrial plant to be inoperative. There are several similar problems in automation systems, so there is the use of the gateway in various processes. It is a technology used in the conversion between protocols, thus being the object of study. The methodology starts with configuring the gateway according to the parameters of the workstation and the robotic manipulator, and then employs the use of the Wireshark® network monitor in order to verify that data sent and received follow the requested specifications.*

Keywords. *ACL, integration, Gateway, Modbus TCP*

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

Introdução. Diversos processos industriais utilizam a conexão entre entradas e saídas dos equipamentos para a integração entre eles. No entanto, essa tecnologia demanda uma quantidade excessiva de cabos e eletrodutos na construção do sistema, visto que cada sinal corresponde a um fio diferente.

Sistemas automatizados mais avançados requerem uma maior quantidade de troca de sinais entre os dispositivos (1). Isso torna inviável a utilização de entradas e saídas na conexão entre os equipamentos, pois dessa forma há um aumento significativo no cabeamento e na infraestrutura. Essa situação ocasionou o surgimento das redes industriais, essa forma permite que os sinais sejam transmitidos via serial, isso proporciona uma redução significativa nos cabos e nos tempos de manutenção.

Apesar dos benefícios proporcionados pelas redes industriais, alguns problemas são encontrados na implementação dessa tecnologia. Os equipamentos devem possuir a mesma lógica no envio e recebimento de dados, ou seja, eles devem seguir o mesmo protocolo. Caso isso não ocorra, eles não conseguem estabelecer a integração. Uma solução bastante implementada na indústria é a conversão das informações.

O *gateway* é um dispositivo capaz de realizar a conexão entre equipamentos de diferentes arquiteturas e protocolos (2). Ele pode ser um *hardware* inserido na rede entre os equipamentos, ou um *software* instalado na própria *workstation* proporcionando a vantagem de não precisar modificar a estrutura física da rede.

Esse artigo propõe a utilização do *gateway Advanced Control Language* (ACL) para Modbus TCP, o qual é um *software* inserido em uma *workstation*. A entidade Modbus Organization, Inc. é a responsável por regulamentar as especificações que regem o protocolo Modbus TCP. Sua função é converter os dados entre os protocolos ACL e Modbus TCP, já que a *workstation* utilizada nos ensaios só é capaz de enviar comandos de rede ACL, porém a comunicação desejada é entre ela e um manipulador robótico Modbus TCP.

Materiais e métodos. O ACL é empregado em robôs da empresa Eshed (3). Os manipuladores realizam as movimentações conforme os comandos ACL recebidos das *workstations*, no entanto, isso restringe a sua aplicação, pois apenas robôs desse mesmo fabricante podem efetuar essa comunicação.

O protocolo Modbus TCP está entre os cinco protocolos com a maior implementação de novos nós em 2018 (4). O manipulador robótico Fanuc® (LR Mate 200iC, São Paulo, 2009) emprega essa forma de comunicação, porém ele não pode ser comandado de forma direta por uma *workstation* ACL. A seguir é mostrada a metodologia para a integração desse sistema, a qual consiste em um *software* instalado na *workstation* realizando a função de *gateway*, e assim convertendo as informações ACL em Modbus TCP. A Figura 1 mostra a topologia do sistema.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

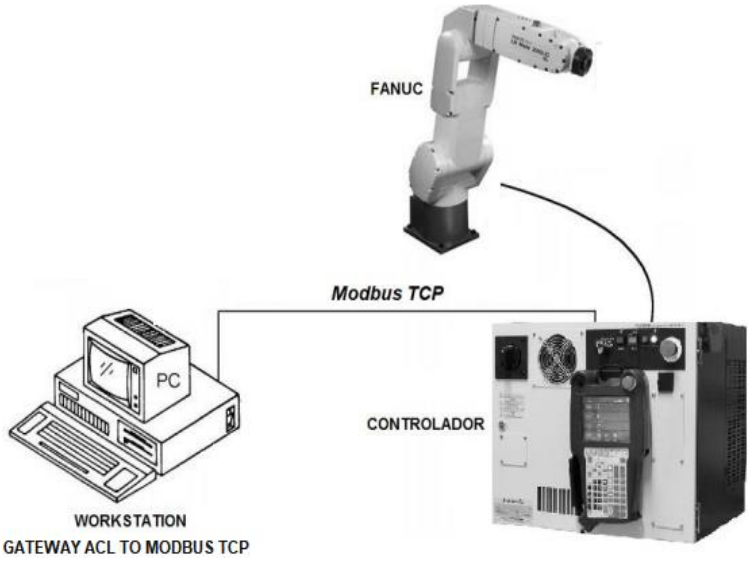

Figura 1. Topologia da rede ACL para Modbus TCP.

A metodologia inicia com a configuração do *gateway* ACL to Modbus TCP na *workstation*. Primeiramente é necessário ter acesso ao computador responsável por todo o processo, o manager. Ele possui toda a documentação do processo, inclusive os endereços das peças (Part ID's) e os locais (ID's) possíveis para os *pick and place's*, os quais devem ser colocados nas configurações do *gateway*, pois assim é possível identificar quais os comandos corretos a serem enviados para o robô. Em seguida, é necessário colocar o endereço de rede *Internet Protocol* (IP) do robô, pois a comunicação utilizada é Ethernet (5), isso significa que o endereçamento é composto por quatro números podendo variar entre 0 e 255.

Conforme mencionado anteriormente, o computador manager é o responsável por gerenciar todas as *workstations* do sistema, além de possuir as informações referentes ao processo, sendo uma delas o modelo tridimensional do sistema com os endereços dos locais e peças, Figura 2. Com a aquisição desses dados é possível configurar o *gateway* ACL to Modbus TCP na *workstation* conforme mostrado na Figura 3.

O *gateway* pode monitorar ou controlar o manipulador robótico, esse processo ocorre através do acesso às memórias do robô utilizando comandos de rede Modbus TCP. Essa ação pode acontecer de duas formas:

- Escrita da memória: o *gateway* modifica os valores alocados dos registradores, dessa forma é possível controlar o robô. Por exemplo, solicitar o momento em que manipulador deve realizar um *pick and place*.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

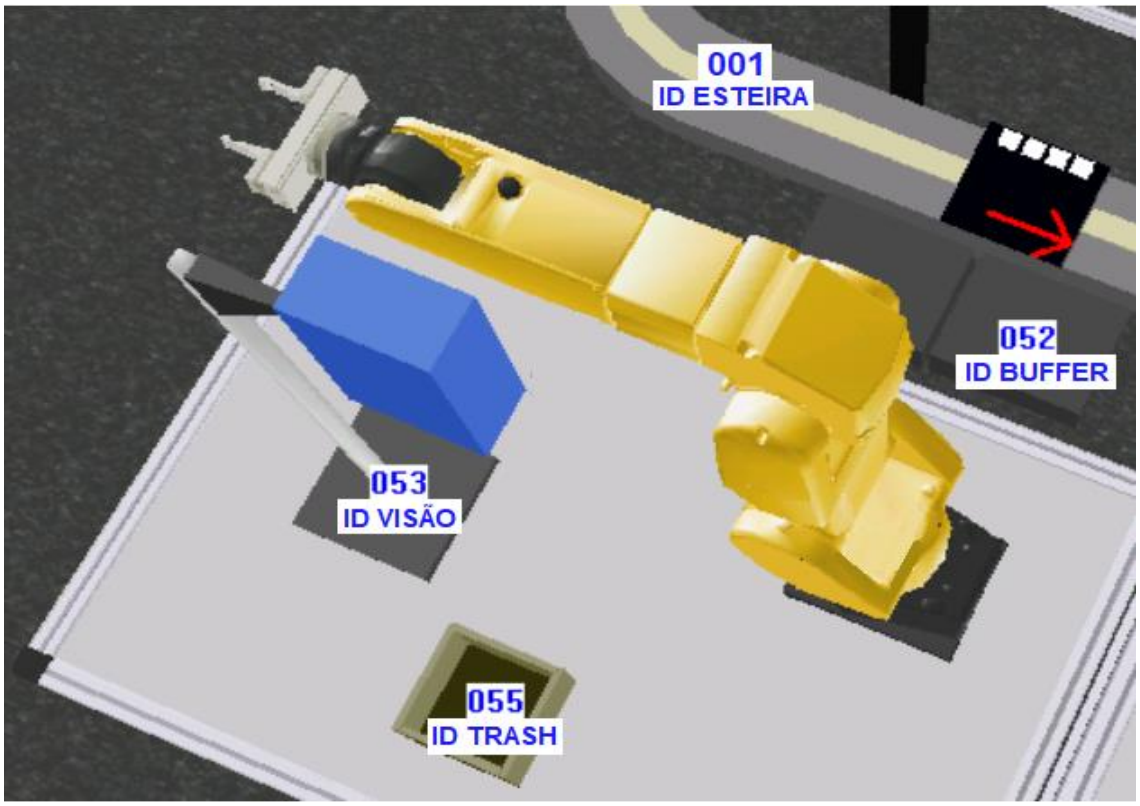

Figura 2. Modelo 3D do sistema com os endereços dos locais para os *pick and place's.*

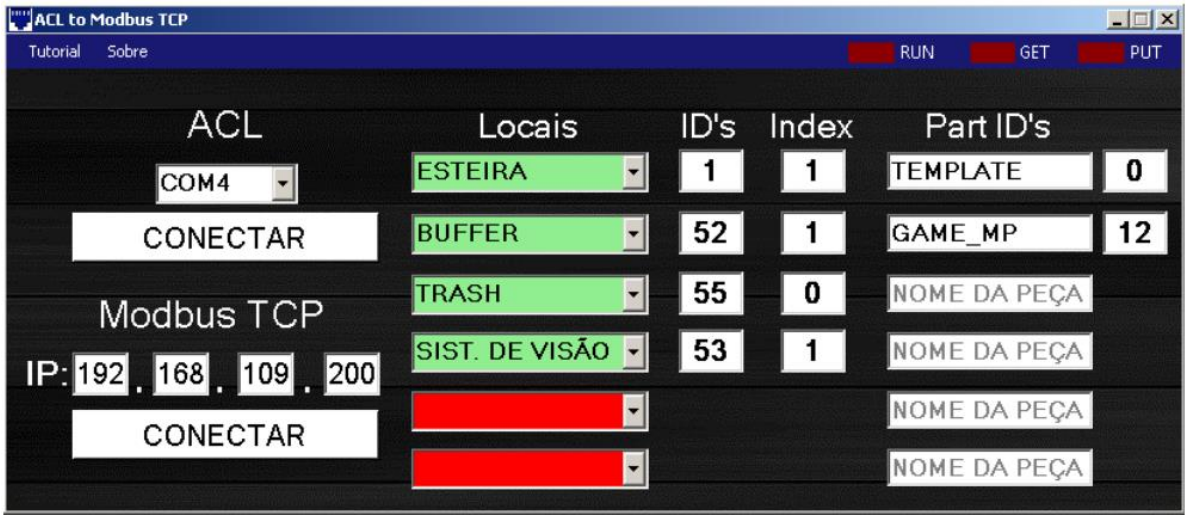

Figura 3. *Gateway* ACL to Modbus TCP configurado conforme os dados do manager.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

- Leitura da memória: o *gateway* verifica quais os valores alocados nos registradores, desse modo é possível monitorar o robô. Por exemplo, averiguar se um *pick and place* foi realizado.

O *gateway* envia comandos de escrita e salva novos valores nos registradores do manipulador de acordo com a tarefa desejada. Os valores dependem dos endereços dos locais para o *pick and place*, ou seja, eles devem seguir a configuração inserida no *gateway*. Dessa forma, o robô compreende qual o trabalho a ser realizado de acordo os ID's e Part ID's inseridos em suas memórias. A Figura 4 mostra o significado desses registradores, sendo que o primeiro é destinado a indicar o início do *pick and place*, os dois posteriores apontam quais são os locais para pegar e soltar a peça, e o último indica o tipo de peça. Além de exibir a definição das memórias do robô, a Figura 4 mostra um exemplo com valores inseridos nos registradores. Nesse exemplo, os números armazenados estão abaixo, é possível observar que a representação numérica utilizada é a binária, pois dessa forma é possível identificar as funções de cada bit ou byte.

- Modo RUN (robô inicia tarefa de *pick and place*) = 2.
- ID da tarefa GET (1º Local para pegar) = 1.
- Index da tarefa GET (2º Local para pegar) = 2.
- ID da tarefa PUT (1º Local para soltar) = 5.
- Index da tarefa PUT (2º Local para soltar) = 1.
- Part ID (Tipo de peça) = 5.

A entidade "Modbus Organization, Inc." é a responsável por regulamentar as especificações que regem o protocolo Modbus TCP, essas normas estão contidas no documento *Modbus Application Protocol Specification v1.1b3* (6). O conteúdo desse material possui a forma com que os pacotes de comunicação devem ser elaborados, dessa forma é possível realizar uma comparação entre os dados enviados pelo *gateway* e as especificações.

O formato oficial do pacote Modbus TCP é visto na Figura 5, cada informação possui a sua descrição abaixo:

- Transação ID: contador de pacotes Modbus TCP já enviados anteriormente.
- Protocolo ID: o valor é sempre 0.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

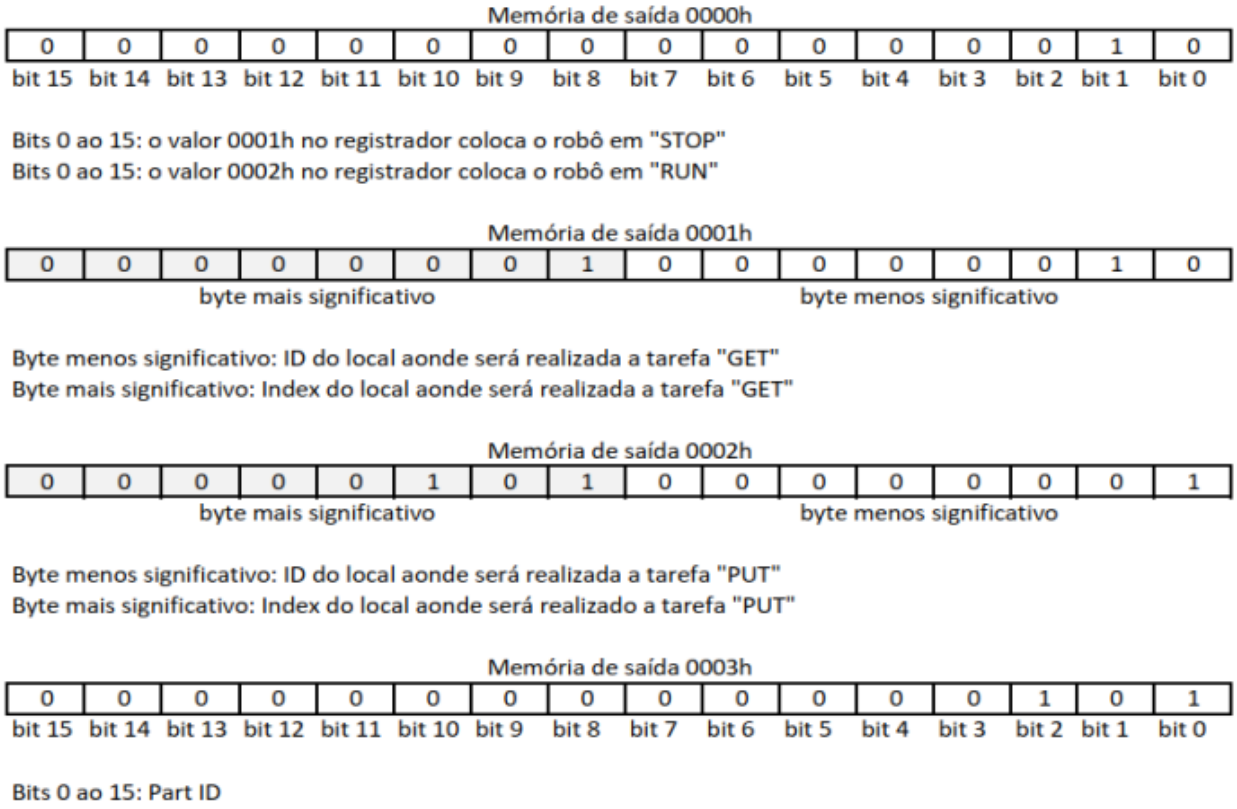

Figura 4. Memórias do manipulador robótico.

- Comprimento: contador de bytes somando os campos Unidade ID, função e variável de dados.
- Unidade ID: endereço do equipamento.
- Função: indica se será feita uma leitura ou uma escrita.
- Dados: contém os dados a serem alocados nos registradores.

Transação ID	Protocolo ID	Comprimento	Unidade ID	Função	Dados
(2 Bytes)	(2 Bytes)	(2 Bytes)	(1 Byte)	(1 Byte)	(Variável)

Figura 5. Pacote Modbus TCP.

Repare que as informações contidas no pacote Modbus TCP atendem a todas especificidades exigidas em uma comunicação, visto que podemos ter acesso a quantidade de comunicações já realizadas anteriormente através do *Transação ID*, verificar o tamanho da

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

informação através do campo *Comprimento*, identificar o equipamento a ser acessado pela *Unidade ID*, indicar se o acesso à memória do dispositivo será para uma leitura ou escrita por meio da *Função*, e solicitar quais os valores a serem alocados nos registradores por intermédio dos *Dados*. Devido a essas características, o protocolo Modbus TCP é um dos mais implementados no meio industrial.

O resultado desse artigo é analisado como uma comparação entre os pacotes enviados do *gateway* para o robô e as especificações oficiais do protocolo Modbus TCP. O ensaio consistiu em diversos pedidos de *pick and place* solicitados ao manipulador, em paralelo a isso, é realizada uma análise das informações.

O monitorador de rede Wireshark é utilizado para essa análise, pois está entre os melhores analisadores de tráfego de dados do mundo (7). Ele é utilizado para mostrar a composição dos pacotes Modbus TCP enviados e recebidos pela *workstation*, além de exibir a quantidade informações trafegadas no decorrer do tempo.

Resultados. A Figura 6 mostra um pacote enviado para o robô pela *workstation*, o qual foi capturado e analisado pelo Wireshark. Com isso, é possível verificar que a construção do pacote segue às especificações do protocolo Modbus TCP mencionadas na Figura 5. O intuito do *gateway* foi solicitar ao manipulador que execute o modo *RUN* (iniciar uma tarefa de *pick and place*). Dessa forma foi necessário alocar o valor 0002h na memória 0000h seguindo a lógica citada anteriormente na Figura 4.

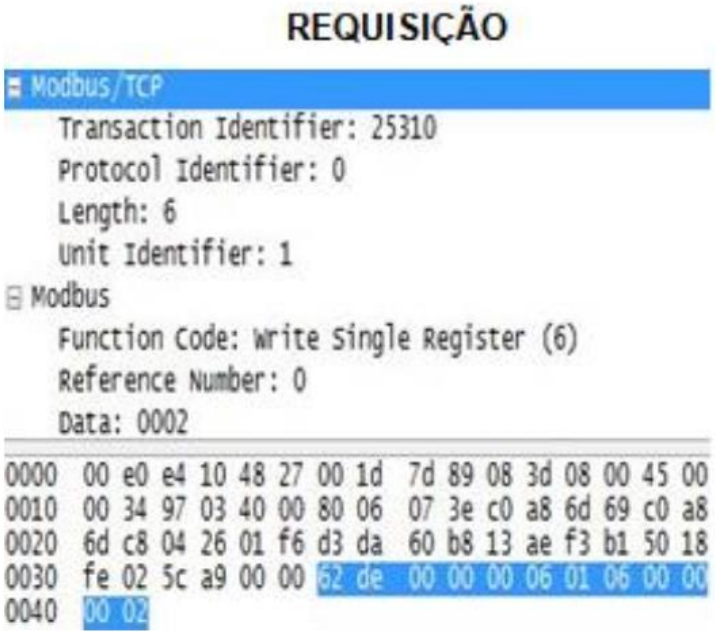

Figura 6. Análise do pacote Modbus TCP pelo Wireshark.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

O Wireshark também foi capaz de gerar um gráfico com o número de pacotes Modbus TCP em função do tempo. Essa informação é de grande valia, visto que ela apresenta a quantidade de informações enviadas e recebidas pelo *gateway*. A Figura 7 mostra que o total de pacotes permaneceu constante na maior parte do tempo, isso indica que o *gateway* é capaz de monitorar o estado do robô de forma ininterrupta, sendo assim confiável. Há apenas oito momentos em que há um aumento no tráfego das informações, são exatamente os instantes em que foram solicitados os *pick and place's*, os quais estão representados na Figura 7 através dos retângulos vermelhos.

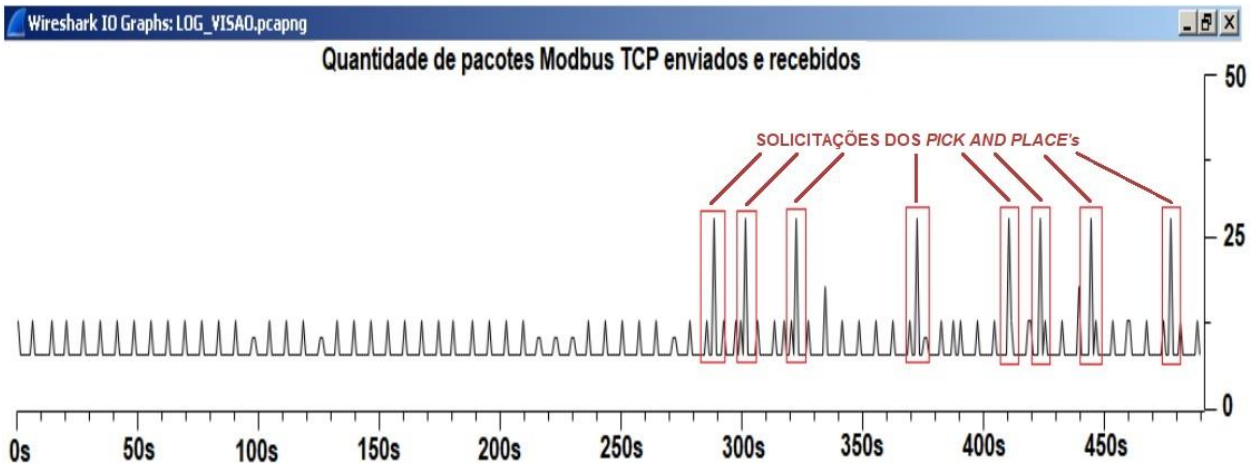

Figura 7. Gráfico de pacotes Modbus TCP em função do tempo.

Conclusão. Ao final dos ensaios, notou-se a eficácia da proposta inicial em empregar o *gateway* ACL to Modbus TCP na conversão dos dados ACL de uma *workstation* para Modbus TCP de um manipulador robótico. A análise do Wireshark mostra que o pacote Modbus TCP enviado ao robô pelo *gateway* segue exatamente as especificações do documento *Modbus Application Protocol Specification v1.1b3*. Ou seja, a comunicação foi executada com êxito com base nas normas vigentes.

As futuras pesquisas relacionadas a esse artigo podem se aprofundar em aplicar técnicas de segurança da informação, pois isso proporcionaria uma maior confiança contra um possível acesso externo não desejado.

Agradecimentos. Os reconhecimentos pelo suporte são destinados ao Instituto Federal de São Paulo (IFSP) e ao SENAI Anchieta.

Divulgação. Os autores declaram não haver conflitos de interesse neste trabalho.

TAS Journal, vol. 4, n. 3, p. 158-166
ISSN 2595-1521
SEPTEMBER 2020
aristotelestecnologo@yahoo.com.br

Referências.

(1) Galloway B, Hancke GP. **Introduction to Industrial**. IEEE Communications Surveys & Tutorials. 2013; p. 860.
(2) IEC 60050. **The World's Online Eletrotechnical Vocabulary**.2010. Disponível em: < http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=732-01-17> Acesso em: 14 jul. 2019.
(3) Eshed. **ACL Reference Guide**.1995. Disponível em: <http://www. Manuals/Robots/Obsolete/Controller_A/100083-a%20ACL44-Ctrl > Acesso em: 02 set. 2019.
(4) Anybus. **Industrial Ethernet is now bigger than fieldbuses**.2018. Disponível em: < https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-biggerthan-fieldbuses > Acesso em: 22 ago. 2019.
(5) Tanenbaum AS. **Computer Networks**. 2003; p. 334.
(6) Modbus.org **Modbus Application Protocol Specification**. 2012. Disponível em: < http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf >. Acesso em: 25 jun. 2019.
(7) Watson J. **2019 Best Packet Sniffers (9 Packet Analyzers Reviewed)**. 2019. Disponível em: < https://www.comparitech.com/net-admin/packet-sniffer-networkanalyzers/>. Acesso em: 19 jun. 2019.