



**UNIVERSIDADE ESTADUAL PAULISTA  
“JÚLIO DE MESQUITA FILHO”  
Campus de Bauru**

**MARCOS ROGÉRIO CALDIÉRI**

**IMPLEMENTAÇÃO DO MODBUS PARA APLICAÇÃO EM SISTEMA DE  
CONTROLE VIA REDE SEM FIO**

Bauru  
2016

MARCOS ROGÉRIO CALDIÉRI

**IMPLEMENTAÇÃO DO MODBUS PARA APLICAÇÃO EM SISTEMA DE  
CONTROLE VIA REDE SEM FIO**

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica da Universidade Estadual Paulista “Júlio de Mesquita Filho” para obtenção do grau de Mestre em Engenharia Elétrica.

**Área de Concentração:** Automação

**Linha de Pesquisa:** Mecatrônica

**Orientador:** Prof. Dr. Eduardo Paciência Godoy

Bauru  
2016

Caldiéri, Marcos Rogério.

Implementação do Modbus para aplicação em sistemas de controle via rede sem fio / Marcos Rogério Caldiéri, 2016

66 f.

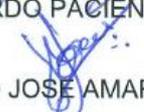
Orientador: Eduardo Paciência Godoy

Dissertação (Mestrado)-Universidade Estadual Paulista. Faculdade de Engenharia, Bauru, 2016

1. Sistema de controle sem fio. 2. PIDPlus. 3. Modbus. I. Universidade Estadual Paulista. Faculdade de Engenharia. II. Título.

**ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE MARCOS ROGERIO CALDIERI, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA, DA FACULDADE DE ENGENHARIA.**

Aos 21 dias do mês de outubro do ano de 2016, às 10:00 horas, no(a) Instituto de Ciência e Tecnologia/UNESP/Sorocaba, reuniu-se a Comissão Examinadora da Defesa Pública, composta pelos seguintes membros: Prof. Dr. EDUARDO PACIÊNCIA GODOY - Orientador(a) do(a) Engenharia de Controle e Automação / Instituto de Ciência e Tecnologia/UNESP/Sorocaba, Prof. Dr. PAULO JOSE AMARAL SERNI do(a) Engenharia de Controle e Automação / Instituto de Ciência e Tecnologia/UNESP/Sorocaba, Professor Doutor MARIO LUIZ TRONCO do(a) Departamento de Engenharia Mecânica / Universidade de São Paulo/São Carlos, sob a presidência do primeiro, a fim de proceder a arguição pública da DISSERTAÇÃO DE MESTRADO de MARCOS ROGERIO CALDIERI, intitulada **IMPLEMENTAÇÃO DO MODBUS PARA APLICAÇÕES DE SISTEMAS DE CONTROLE VIA REDES SEM FIO**. Após a exposição, o discente foi arguido oralmente pelos membros da Comissão Examinadora, tendo recebido o conceito final: APROVADO. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelos membros da Comissão Examinadora.

  
Prof. Dr. EDUARDO PACIÊNCIA GODOY  
Prof. Dr. PAULO JOSE AMARAL SERNI  
Professor Doutor MARIO LUIZ TRONCO

## RESUMO

A recente introdução de transmissores sem fio na indústria provocou um novo interesse em técnicas de medição e controle, porém a maioria das aplicações está restrita a medições de variáveis de processo em malha aberta ou aplicações de monitoramento. O motivo é a falta de confiabilidade devido aos problemas inerentes ao meio de transmissão, que pode ser a perda de pacotes de informação, atrasos de comunicação variantes no tempo, atualização muito lenta e não periódica da medição e vários tipos de interferências. A maior parte dos controladores industriais em controle de processos assumem que o ciclo de controle é executado de forma periódica e que uma nova medição está disponível para ser usada em intervalos de tempo conhecidos. No entanto esta situação não pode ser garantida quando sensores ou transmissores sem fio são usados em aplicações de controle em malha fechada, denominadas de Sistemas de Controle via Redes sem fio (WNCS – Wireless Networked Control Systems). Nesses tipos de aplicações, os transmissores sem fio devem transmitir novas medições de forma não periódica e somente se a medição da variável do processo tiver alterado significativamente. Para tornar esta tecnologia de WNCS mais confiável, muitas técnicas de controle têm sido pesquisadas, entre elas o PIDPlus que representa uma modificação do algoritmo PID para controle via rede sem fio. Este trabalho apresenta a implementação do protocolo Modbus para aplicações de WNCS. O protocolo Modbus TCP foi embarcado em hardware dedicado viabilizando a transmissão de dados via Ethernet TCP/IP e Wi-Fi. Uma comparação e avaliação de controladores PID para aplicação em WNCS sob condições de amostragem e atrasos de comunicações variáveis e de perdas de transmissão de mensagens foi realizada. Os resultados são analisados do ponto de vista de desempenho de controle e robustez. Resultados experimentais numa planta piloto comprovam a eficiência da implementação de uma malha de controle sem fio usando uma rede Wi-Fi com o protocolo Modbus embarcado e um controlador PIDPlus.

**Palavras-chave:** Sistemas de Controle via Redes Sem Fio, PIDPlus, Modbus.

## ABSTRACT

The recent introduction of wireless transmitters in the industry has driven a new interest in measuring and control techniques, but most applications are restricted to measurements of process variables in open loop or monitoring applications. The reason is the lack of reliability due to problems inherent to the transmission medium, which may be the packet loss, time varying delay, slow and aperiodic measurement updates and interference. Most industrial process controllers assume that the control cycle is performed periodically and that a new measurement is available to be used at known time intervals. However it cannot be guaranteed when wireless sensors or transmitters are used in closed loop control applications, called Wireless Networked Control Systems (WNCS). In these type of applications, wireless transmitters shall transmit new measurements not periodically and only if the process variable measurement has changed significantly. In order to enable and make this WNCS technology reliable, many control techniques have been researched including the PIDPlus that is a modified PID algorithm for wireless control. This paper presents the implementation of the Modbus protocol for WNCS applications. The Modbus TCP was embedded in dedicated hardware enabling the transmission of data via Ethernet TCP/IP and Wi-Fi. A comparison and evaluation of PID controllers for WNCS were done considering situations of variable sampling and communication delays and packet losses. The results are analyzed from the point of view of control performance and robustness. Experimental results in a pilot plant prove the efficiency of the implementation of a wireless control loop using a Wi-Fi network with embedded Modbus protocol and PIDPlus controller.

**Keywords:** Wireless Networked Control Systems, PIDPlus, Modbus.

## LISTA DE FIGURAS

Figura 1: Estrutura de um Sistema de Controle via Rede (NCS) .....	16
Figura 2: A classificação das aplicações de automação industrial .....	20
Figura 3: Estrutura de uma Mensagem Modbus.....	24
Figura 4: Modelo de mensagem (query) Modbus .....	25
Figura 5: Framing modo ASCII .....	27
Figura 6: Framing modo RTU .....	27
Figura 7: Estrutura de uma Mensagem Modbus TCP/IP.....	32
Figura 8: Implementação do Modbus WiFi.....	38
Figura 9: Conjunto do Arduino com shield XBee e Ethernet .....	39
Figura 10: Shield XBee .....	39
Figura 11: Shield Ethernet.....	40
Figura 12: XBee WiFi .....	41
Figura 13: Fluxograma da rotina principal e da sub-rotina de recebimento de mensagens Modbus .....	43
Figura 14: Fluxograma da sub-rotina de interpretação da solicitação Modbus.....	44
Figura 15: Fluxograma da sub-rotina de resposta Modbus .....	45
Figura 16: Diferença entre mensagem Modbus RTU e Modbus TCP/IP.....	46
Figura 17: Mensagem Modbus RTU .....	46
Figura 18: Mensagem Modbus TCP.....	47
Figura 19: Planta Piloto de Processos – SENAI Lençóis Paulista .....	47
Figura 20: Diagrama P&ID do processo em estudo .....	48
Figura 21: Ligação elétrica do medidor de vazão magnético e transmissor de rede Wi-Fi .....	49
Figura 22: Instalação do medidor de vazão magnético e transmissor de rede Wi-Fi.....	50
Figura 23: Coleta das informações de vazão e processamento. ....	50
Figura 24: Blocos de funções Modbus. ....	51
Figura 25: Tela gráfica dos comandos e das variáveis do controle. ....	51
Figura 26: Ligação elétrica entre Arduino e Inversor de Frequência. ....	52
Figura 27: Instalação do Arduino e Inversor de Frequência .....	52
Figura 28: Arquitetura do WNCS com redes Modbus .....	53
Figura 29: Estrutura do controlador PIDPlus .....	54
Figura 30: Histograma do tempo de atraso da rede Modbus Wi-Fi .....	57

Figura 31: Controle de vazão utilizando o PID e PIDPlus .....	58
Figura 32: Controle de vazão: PID e PIDPlus com falhas de comunicação.....	59
Figura 33: Controle de vazão: PIDPlus com falhas de comunicação aleatória.....	60
Figura 34: Controle de vazão: PIDPlus e PID tradicional com falhas de comunicação sequencial 30x6 e 15x6 .....	61
Figura 35: WNCS de vazão: Impacto do período de amostragem do sensor sem fio na resposta .....	63
Figura 36: Controle de vazão: PIDPlus com atraso de comunicação variável.....	64

## LISTA DE TABELAS

Tabela 1: Exceptions .....	29
Tabela 2: Parâmetros para protocolos sem fio.....	35
Tabela 3: Recursos disponíveis na planta piloto .....	49
Tabela 4: Desempenho da rede sem fio no controle PID. ....	57
Tabela 5: Desempenho dos controladores PID e PIDPlus. ....	60
Tabela 6: Desempenho do controlador PIDPlus com falhas de comunicação aleatória .....	61
Tabela 7: Desempenho dos controladores com falhas de comunicação sequencial 30x6 e 15x6 .....	62
Tabela 8: Desempenho do WNCS variando o período de amostragem do sensor sem fio .....	63

## LISTA DE ABREVIATURAS E SIGLAS

<b>ADU</b>	<i>Application Data Unit</i>
<b>ASCII</b>	<i>American Standard Code for Information Interchange</i>
<b>CLP</b>	<i>Controladores Lógicos Programáveis</i>
<b>CRC</b>	<i>Cyclical Redundancy Check</i>
<b>CSMA/CD</b>	<i>Carrier Sense Multiple Access com Collision Detect</i>
<b>DCF</b>	<i>Distributed Control Function</i>
<b>IAE</b>	<i>Integral of Absolute Error</i>
<b>ITAE</b>	<i>Integral Time-weighted Absolute Error</i>
<b>LRC</b>	<i>Longitudinal Redundancy Check</i>
<b>MAC</b>	<i>Medium Access Control</i>
<b>MBAP</b>	<i>Modbus Application Protocol</i>
<b>NCS</b>	<i>Networked Control System</i>
<b>OEM</b>	<i>Original Equipment Manufacturer</i>
<b>OSI</b>	<i>Open Systems Interconnection</i>
<b>OFDM</b>	<i>Orthogonal Frequency Division Multiplexed</i>
<b>P&amp;ID</b>	<i>Pipe and Instrumentation Diagram</i>
<b>PID</b>	<i>Proportional, Integral e Derivative</i>
<b>PDU</b>	<i>Protocol Data Unit</i>
<b>PoE</b>	<i>Power over Ethernet</i>
<b>RTU</b>	<i>Remote Terminal Unit</i>
<b>SPI</b>	<i>Serial Peripheral Interface</i>
<b>TCP/IP</b>	<i>Transmission Control Protocol</i>
<b>UART</b>	<i>Universal Asynchronous Receiver/Transmitter</i>
<b>WLAN</b>	<i>Wireless Local Area Network</i>
<b>WNCS</b>	<i>Wireless Networked Control System</i>
<b>WPA</b>	<i>Wi-Fi Protected Access</i>
<b>WPAN</b>	<i>Wireless Personal Area Network</i>

## SUMÁRIO

<b>1. INTRODUÇÃO</b> .....	12
1.1 JUSTIFICATIVA .....	12
1.2 OBJETIVOS .....	14
<b>2. REVISÃO BIBLIOGRÁFICA</b> .....	15
2.1 SISTEMA DE CONTROLE VIA REDE SEM FIO .....	15
2.2 APLICAÇÕES DE WNCS .....	21
<b>3. REVISÃO CONCEITUAL</b> .....	23
3.1 PROTOCOLO MODBUS .....	23
3.1.1 MODBUS TCP .....	31
3.1.2 MODBUS WI-FI – WI-FI 802.11 .....	33
3.2 DETERMINISMO .....	35
<b>4. MATERIAIS E MÉTODOS</b> .....	38
4.1 IMPLEMENTAÇÕES DO MODBUS .....	38
4.2 BANCADA DE WNCS .....	47
4.3 ESTRATÉGIA DE CONTROLE .....	53
<b>5. RESULTADOS E DISCUSSÕES</b> .....	56
5.1 MÉTRICAS DE DESEMPENHO DO MODBUS WI-FI .....	56
5.2 COMPARAÇÃO DE CONTROLADORES .....	57
5.3 DESEMPENHO DO WNCS SOB CONDIÇÕES DE FALHAS DE COMUNICAÇÃO DE FORMA ALEATÓRIA E SEQUENCIAL .....	60
5.4 DESEMPENHO DO WNCS SOB VARIAÇÃO DO PERÍODO DE AMOSTRAGEM DO SENSOR SEM FIO .....	62
5.5 DESEMPENHO DO WNCS SOB VARIAÇÃO DO ATRASO DE COMUNICAÇÃO .....	64
<b>6. CONCLUSÃO</b> .....	65
<b>7. REFERÊNCIAS</b> .....	66

## 1. INTRODUÇÃO

No cenário industrial moderno, os processos de produção estão sujeitos a diversas restrições, que englobam aumento da rentabilidade, otimização dos recursos (e.g. matéria-prima, suprimento de energia), exigências de segurança e o comprometimento com as regulamentações socioambientais. Tais restrições implicam na necessidade de conhecimento qualitativo e quantitativo do processo e de seus parâmetros. Portanto, aplicar um sistema de medições, monitoramento e controle adequado é um aspecto importante.

O conceito de redes industriais fornece muitos benefícios, acima de tudo, uma maior flexibilidade e modularidade de instalações e a facilidade de configuração do sistema, comissionamento e manutenção (GALLOWAY & HANCKE, 2013). De acordo com Sauter (2010), as redes de controle industrial podem ser divididas em três gerações distintas, com diferentes níveis de compatibilidade. A primeira consiste em protocolos seriais *fieldbus* tradicionais, o segundo de protocolos baseados em Ethernet e a última geração, que começou a incorporar a tecnologia de comunicação wireless.

Aplicações recentes de sistemas de controle distribuído demonstram o surgimento de uma nova abordagem para a utilização de redes industriais. Nessa abordagem, o controlador e a planta ficam fisicamente separados e são conectados por uma rede de comunicação. Este tipo de implementação em sistemas onde as malhas de controle são fechadas sob uma rede de comunicação industrial tem sido denominado de Sistema de Controle via Redes (NCS – *Networked Control System*) (GUPTA & CHOW, 2010).

### 1.1 JUSTIFICATIVA

Avanços recentes na tecnologia de redes de sensores sem fio levaram ao desenvolvimento de dispositivos de baixo custo e baixo consumo de energia. Com esses avanços, uma nova tendência surgiu com o uso de redes sem fio em NCS (FISCHIONE et al., 2011), promovendo interoperabilidade entre redes com fio já existentes e novas redes sem fio. Estes sistemas são conhecidos como sistemas de controle via redes sem fio (WNCS - *Wireless Networked Control Systems*). Os WNCSs ultimamente têm atraído muitos esforços de pesquisa e desenvolvimento, conduzidos principalmente pela crescente evolução e padronização de redes sem fio como ZigBee, Wi-Fi (PAAVOLA & LEIVISKA, 2010), Wireless Hart e ISA-100.11a (PETERSEN & CARLSEN, 2011).

Muitas características interessantes inerentes às redes sem fio estão motivando o desenvolvimento de WNCS. Os sistemas sem fio proporcionam vantagens como (GALLOWAY & HANCKE, 2013):

- a redução na quantidade de fiação necessária para a comunicação, que por sua vez reduz os custos da instalação;
- o comissionamento e a reconfiguração podem ser realizadas com mais rapidez;
- o instalação preferencial em equipamentos que se movimentam onde o cabeamento pode ser facilmente danificado;
- em ambientes perigosos e instalações de segurança intrínseca;
- em localidades onde cabos podem restringir o funcionamento das máquinas a serem monitoradas e;
- em ambientes com longas distâncias entre dispositivos e de difícil acesso como em refinarias ou de outras plantas de processamento.

A aplicação de redes sem fio tem sido um tema de pesquisa desafiador por um longo tempo e ainda está longe de se esgotar. Neste momento não é de se esperar que as redes sem fio substituam completamente as redes de automação com fio. Pelo contrário, as redes sem fio irão complementar os sistemas atuais. O WNCS pode ser operado entre os sistemas com fio e sem fio existentes e também proporciona vantagens em relação a potência e flexibilidade quando comparados aos com fio formando uma rede híbrida (NAGHSHTABRIZI & HESPANHA, 2011).

Esta introdução de transmissores e atuadores sem fio na indústria de processo provocou um novo interesse em técnicas que podem ser usadas para permitir que o controle em malha fechada seja usado com atualizações de informação não periódicas (BLEVINS et. al, 2014). Uma condição essencial para o controle de processo sempre foi que o controle é executado em uma base periódica e que um novo valor de medição está disponível para cada execução. No entanto, para minimizar o consumo de energia de um transmissor sem fio, os valores de medição podem ser transmitidos com uma frequência baixa, ou somente se o valor da medição mudar significativamente (BLEVINS et al., 2014). Desta forma o controle tem que ser modificado para trabalhar com atualizações não periódicas de medição. Além disso, é importante que a perda de comunicação seja tratada automaticamente pelo controle de uma forma a não introduzir uma interrupção do processo.

Quando a medição não é atualizada em uma base periódica, um PID tradicional não é indicado, pois as ações de controle não serão calculadas de forma correta. Se o controle é executado apenas quando uma nova medida é informada, isso poderia resultar em um atraso na resposta de um controlador. Assim, um desafio tem sido a proposta de uma técnica que minimize a frequência de medição de uma variável sem comprometer o desempenho do controle. Para resolver estas questões o algoritmo PID pode ser modificado para funcionar corretamente com atualizações de medição lentas, não periódica e perda de comunicação. Por exemplo, o PIDPlus oferece um PID modificado para controle em malha fechada, usando um transmissor de rede sem fio (BLEVINS et al., 2014).

## 1.2 OBJETIVOS

Avaliar e comparar o desenvolvimento de WNCS usando o protocolo de comunicação industrial Modbus e controladores PID. O protocolo Modbus TCP foi implementado para a transmissão de dados via Ethernet TCP/IP (controlador – atuador) e Wi-Fi (sensor – controlador). Os controladores PID e PIDPlus são analisados.

## 2. REVISÃO BIBLIOGRÁFICA

### 2.1 SISTEMA DE CONTROLE VIA REDE SEM FIO

Nas últimas décadas, o aumento da eficiência e o baixo custo dos componentes eletrônicos influenciaram os sistemas de controle industrial. Inicialmente, o controle de plantas e processo de fabricação era manual, ocasionando baixa produtividade e alto custo. O primeiro trabalho significativo de controle automático foi o regulador centrífugo elaborado por James Watt no século XVIII destinado ao controle de máquinas a vapor. O grande avanço na teoria de controle nas décadas de 20 e 30 impulsionou o desenvolvimento dos primeiros controladores PID comerciais. Na década de 30 e 40 os controladores PID pneumáticos dominaram o mercado. Na década de 50 surgiram as primeiras versões eletrônicas de controle empregando transdutores, relés e circuitos de controle. Estas versões eram implementadas a partir de amplificadores operacionais. No início da década de 60 surgiram as primeiras aplicações em controle de processos baseadas em computadores. Com o surgimento do circuito integrado e microprocessadores, a funcionalidade de múltiplas malhas de controle analógicos pode ser replicada para um único controlador digital. Controladores digitais começaram a substituir continuamente o controle analógico, embora a comunicação para o campo ainda fosse realizada usando sinais analógicos. Tecnologias como microcontroladores programáveis e processadores de sinais digitais permitiu a substituição de malhas de controle puramente analógicos por controladores digitais, tais como CLPs (Controladores Lógicos Programáveis). A partir da década de 80 as versões digitais de controladores PID dominaram o mercado e tiveram um grande impacto no controle de processos em virtude de sua versatilidade e facilidade de implementação.

A tendência de migração dos controles para os sistemas digitais resultou na necessidade de novos protocolos de comunicação para controladores e instrumentos de campo. Estes protocolos de comunicação são comumente conhecidos como protocolos *Fieldbus*. Existem vários protocolos de comunicação, cada um com suas particularidades que vão atender a todos os setores, como a indústria de manufatura, alimentícia, petrolífera, geração de energia, transporte, tratamento de água, automotiva, entre outras.

Desde meados da década de 1980, quando a automação deu um grande salto com as operadoras de linha de energia com sensores e atuadores mais inteligentes, uma espécie de corrida do ouro foi estabelecida. Neste momento, muitos sistemas *Fieldbus* nasceram e foram adaptados para diferentes campos de aplicação, e quase todas as empresas no ramo de automação criaram seu próprio protocolo. Do ponto de vista tecnológico, a evolução real dos

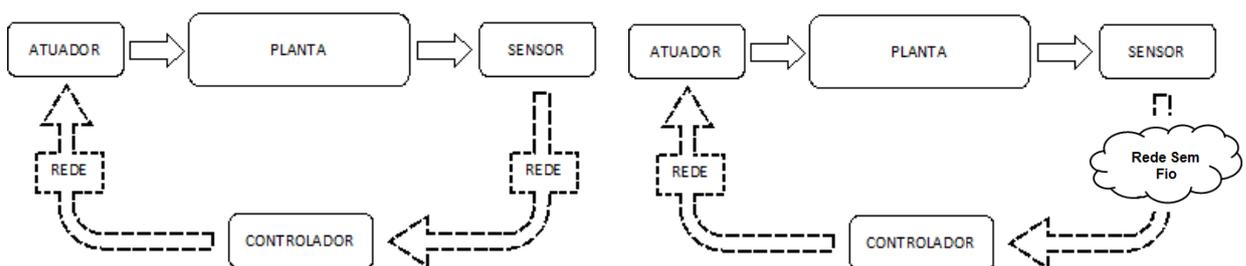
sistemas *Fieldbus*, foi fortemente influenciada pelo desenvolvimento de redes de computadores.

A demanda por uma redução de peso de cabeamento em aviônicos e tecnologia espacial levou ao desenvolvimento do barramento 1553 de padrão militar, que pode ser considerado como o primeiro *Fieldbus*. Lançado em 1970, mostrou muitas propriedades características dos sistemas *Fieldbus* modernas:

- a transmissão serial de controle e informação de dados sobre a mesma linha;
- estrutura mestre-escravo;
- possibilidade de cobrir longas distâncias e;
- controladores integrados.

Mais tarde, os propósitos semelhantes (redução do peso cabeamento e custos) resultaram no desenvolvimento de vários barramentos, não só na indústria automobilística, mas também na área de automação. Nos últimos 15 anos, os sistemas *Fieldbus* têm exigido muito trabalho para definição, especificação, implementação e difusão no mercado. Hoje em dia, os sistemas *Fieldbus* são padronizados e amplamente utilizados na automação industrial (THOMESSE, 1999). O conceito de rede fornece muitos benefícios, acima de tudo, uma maior flexibilidade e modularidade de instalações ou a facilidade de configuração do sistema, comissionamento e manutenção (THOMESSE, 1999). As informações que são transmitidas em redes industriais são para controle, informações de diagnóstico e segurança, como pode ser visto na Figura 1.

Figura 1: Estrutura de um Sistema de Controle via Rede (NCS)



Fonte: Godoy et al. (2013)

Informações de controle são enviadas entre os instrumentos e controladores. Informações de diagnóstico é uma informação sensorial que pode ser utilizada pelo sistema de controle. Esta informação é geralmente utilizada para monitorar o estado de equipamentos em uma planta

industrial. Informações de segurança são usadas para implementar funções críticas, tais como o fechamento seguro de um equipamento e a operação de circuitos de proteção. Portanto, para esta informação o requisito tempo real é muito importante.

Os sistemas de controle em rede possuem alguns problemas inerentes a aplicações de controle que não existiam em sistemas analógicos e que são normalmente difíceis de serem detectados devido às variações e incertezas introduzidas pela rede de comunicação, como: atrasos, instabilidade, limitações de largura de banda e perda de pacotes (BAILLIEUL et al., 2007). Um consenso na pesquisa sobre Sistemas de Controle em Rede (NCS – *Network Control System*) é que a presença dessas imperfeições e restrições relativas à rede de comunicação pode afetar significativamente o desempenho da malha de controle, podendo até torná-lo instável, como demonstrado por Cloosterman et al. (2009). Portanto, o principal desafio na NCSs é entender como esses fatores afetam o desempenho e a estabilidade do sistema, de preferência de forma quantitativa, e destacar os fatores mais importantes para cada tipo de NCS (HEEMELS et al., 2010).

De acordo com Sauter (2010), as redes de controle industrial podem ser divididas em três gerações distintas, com diferentes níveis de compatibilidade: A primeira consiste em protocolos seriais *Fieldbus* tradicionais, o segundo de protocolos baseados em Ethernet e a última geração, que incorpora a tecnologia de comunicação sem fio. As redes de sensores sem fio tem sido objeto de intensa pesquisa. Elas têm o potencial de revolucionar diversos segmentos da economia e atividades por meio de aplicações que vão desde o monitoramento ambiental e agrícola, controle de processos industriais, transportes e aplicações em redes inteligentes de energia.

A aplicação de redes sem fio tem sido um tema de pesquisa desafiador por um longo tempo e ainda está longe de se esgotar. Neste momento não é de se esperar que as redes sem fio substituam completamente as redes de automação com fio, em vez disso, eles vão complementá-los sempre que necessário. O Sistema de Controle via Rede sem Fio (WNCS – *Wireless Network Control System*) pode ser operado entre os sistemas com fio e sem fio existentes e também proporciona vantagens em relação a potência e flexibilidade quando comparados aos com fio formando uma rede híbrida (NAGHSHTABRIZI et al., 2011).

Os nós sensores são fisicamente pequenos e normalmente fornecidos com transmissores e receptores de rádio, microcontroladores, baterias e pilhas (LOW et al., 2005.). Os nós incluem a capacidade de comunicação sem fio, bem como recursos de computação suficientes para processamento de sinal e de transmissão de dados (AAKVAAG et al., 2005). Dependendo do ambiente circundante, a comunicação WNCS pode ser implementada de diversas maneiras. Por

isso, várias topologias de rede são possíveis: estrela, conjunto-árvore e malha. Nestas topologias, nós sensores podem agir como um simples transmissores de dados e receptores ou roteadores que trabalham em uma forma *ad-hoc*.

A introdução de transmissores sem fio na indústria provocou um novo interesse em técnicas de medição e controle, porém a maioria das aplicações está restrita a medições de variáveis de processo em malha aberta ou aplicações de monitoramento. O motivo é a falta de confiabilidade devido aos problemas inerentes ao meio de transmissão, que pode ser à perda de pacotes de informação, atrasos de comunicação variantes no tempo, atualização muito lenta e não periódica da medição e vários tipos de interferências. No entanto, percebe-se uma demanda por técnicas de controle que podem ser usadas para permitir que o controle em malha fechada seja eficaz usando atualizações de informações periódicas ou não periódicas (BLEVINS et al., 2014).

A maior parte dos controladores industriais de processos assumem que o ciclo de controle é executado de forma periódica e que uma nova medição está disponível para ser usada em intervalos de tempo conhecidos. No entanto, esta situação não pode ser garantida quando sensores ou transmissores sem fio são usados em aplicações de controle em malha fechada, como os WNCS. Nesses tipos de aplicações, os transmissores sem fio devem transmitir novas medições de forma não periódica e somente se a medição da variável do processo for alterada significativamente.

Um problema mais recente e importante requisito tecnológico para a aplicação de WNCS é a eficiência energética dos dispositivos (ARAÚJO et al., 2014), pois como são alimentados por baterias, espera-se o menor consumo possível para estender a vida útil da bateria. Devido à igualdade de tecnologia entre os fabricantes de sensores sem fio industrial, a vida útil da bateria tornou-se um recurso para distinguir produtos. No entanto, reduzir o consumo de energia em WNCS pode ser um desafio devido à exigência por rápidas atualizações dos atuais sistemas de controle digital. Portanto, a pesquisa sobre estratégias de controle focadas na redução do gasto energético para aplicações de WNCSs tem ganhado importância (SADI et al., 2014; LI et al., 2014).

Os principais padrões de comunicação sem fio mais utilizados na indústria são: WLAN 802.11, Bluetooth WPAN 802.15.1, 802.15.4 e ZigBee. Estes protocolos funcionam na banda ISM de 2,4 GHz, e podem coexistir em implantações industriais atuais (MILLAN et al, 2011). Em WNCS, há uma tendência em utilizar padrões de tecnologias existentes para transmissão de informações, além de soluções proprietárias específicas. A indústria favorece padrões sem

fio, pelo menos, para as camadas inferiores do protocolo. As tecnologias sem fio atualmente mais utilizadas são as seguintes:

- IEEE 802.11 [LAN sem fio (WLAN)] em suas muitas aplicações, este é o padrão, que das redes sem fio na área de escritório é visto como uma extensão sem fio natural de Ethernet. Portanto, é também empregado no campo de automação.
- IEEE 802.15.4 [rede de área pessoal (WPAN)], em especial com camadas de protocolo adicionais mais elevados de ZigBee. Este é o candidato mais promissor para redes de sensores sem fio, devido a sua capacidade de economia de energia e, portanto, particularmente interessante para automação predial. É também a base para o Wireless HART -ISA 100.11a que tem um padrão mais abrangente e que ainda está em construção.
- IEEE 802.15.1 (Bluetooth) é amplamente utilizado em automação industrial, embora a versão 1 está limitado a redes de curto alcance. No entanto, a próxima versão 2 vai superar a restrição de faixa.
- IEEE 802.16 [Interoperabilidade Mundial para Acesso por Micro-ondas (WiMAX)] é um padrão de banda larga que se destina a cobrir as redes de longo alcance. No momento não é amplamente aplicada na automação, mas pode ser interessante no futuro.
- UWB (banda ultra larga, anteriormente IEEE 802.15.3a) é um conjunto de tecnologias de camada física que fornecem altas taxas de dados para redes de curto alcance. A situação atual da padronização não é clara, podendo então, tornar-se interessante na forma de *wireless Universal Serial Bus* (USB) e Bluetooth 3.0 (SAUTER, 2010).

Do ponto de vista industrial, o grupo de trabalho da norma ISA SP100 apresentou seis classes para comunicações sem fios. As classes foram baseadas na análise de aplicações de comunicações sem fios industriais entre dispositivos (ISA-SP100.11a, 2006).

- Classe 5 define itens relacionados ao monitoramento sem consequências operacionais imediatas. Esta categoria inclui as aplicações sem o critério de prontidão forte. A exigência de confiabilidade pode, no entanto, variar. Alguns, como logs de sequência-de-eventos, exigem alta confiabilidade; outros, como relatórios de mudança lenta e informações de baixo valor econômico, não precisam ser tão confiáveis, já que a perda de algumas amostras consecutivas, pode não ser importante. (ISA-SP100.11, 2006).

- Classe 4 define o acompanhamento com consequências operacionais de curto prazo, que inclui limite alto e limite baixo de alarmes e outras informações que podem necessitar de maior corrente ou envolvimento de um técnico de manutenção. Atualizações das informações nesta classe são tipicamente baixas (lenta), medida em minutos ou mesmo em horas. (ISA-SP100.11, 2006).
- Classe 3 abrange as aplicações de controle de malha aberta, na qual um operador, em vez de uma máquina, fecha o ciclo entre entrada e saída. Por exemplo, um operador poderia tomar uma unidade fora de linha, se necessário. Oportunidade para esta classe é a escala humana, medida de segundos a minutos. (ISA-SP100.11, 2006)
- Classe 2 consiste de controle de supervisão de malha fechada, cujas aplicações geralmente têm constantes de tempo longas, com pontualidade das comunicações medidas de segundos a minutos. Exemplos desta categoria são unidade de lotes e seleção de equipamentos. (ISA-SP100.11, 2006)
- Classe 1, controle em malha fechada, inclui controle de velocidade, vazão e pressão, que possuem uma dinâmica rápida. A atualização das informações nesta classe é muitas vezes crítica. (ISA-SP100.11, 2006)
- Classe 0 define ações de emergência relacionadas com a segurança, que são sempre críticas, tanto para pessoas como para as instalações. A maioria das funções de segurança são, e serão, realizadas por redes com fio dedicadas a fim de limitar os modos de falha e vulnerabilidade a eventos ou ataques externos. Exemplos desta categoria são de bloqueio de segurança, o desligamento de emergência e controle de incêndio. (ISA-SP100.11, 2006)

Figura 2: A classificação das aplicações de automação industrial

Segurança	Classe 0: Ações de emergência Sempre crítico
Controle	Classe 1: Ajustes de Controle em Malha Fechada Frequentemente crítico
	Classe 2: Supervisão de Controle em Malha Fechada Usualmente não crítico
	Classe 3: Controle em Malha Aberta Humano no controle da malha
Monitoramento	Classe 4: Alerta Consequência operacional de curto prazo
	Classe 5: Visualização de valores Sem consequências operacionais imediatas

Fonte: (ISA-SP100.11, 2006)

## 2.2 APLICAÇÕES DE WNCS

Para fornecer recursos de monitoramento remoto sem fio para controladores industriais, tais como CLPs, uma solução simples que tem sido aplicada é o uso de dispositivos conversores serial - sem fio. Estes dispositivos são interfaces eletrônicas que recebem dados de conexões seriais, bastante comum em dispositivos industriais e retransmite-o através de conexões sem fio.

De acordo com Fischione et al. (2011), a aplicação mais comum de redes sem fio é principalmente para monitoramento. A confiabilidade é muito relacionada com as perdas de pacotes ou até mesmo mensagens transmitidas na rede que não foi corrigida. Tipicamente, as perdas de pacotes resultam de erros de transmissão em links de rede física ou de estouros de *buffer* devido ao congestionamento. Além disso, em aplicações de monitoramento não há rígidas restrições de tempo sobre a entrega destas mensagens, uma vez que o intervalo de amostragem é normalmente dado em segundos para garantir uma grande vida útil da bateria (PAAVOLA et al, 2010).

Por outro lado, quando as redes sem fio são utilizadas para aplicações em controle, tais como em WNCS, outros fatores devem ser considerados. Ao contrário das aplicações de monitoramento, WNCS não precisa maximizar a confiabilidade. Hespanha et al. (2007) apresenta alguns resultados sobre o desenvolvimento de NCS para superar os efeitos perdas de pacotes no seu desempenho e estabilidade. De acordo com (NAGHSHTABRIZI et al, 2011), os fatores adicionais que precisam ser considerados para a implementação WNCS, estão o tempo de atraso, o *jitter*, capacidades de transmissão em tempo real e a limitação da largura de banda.

A transmissão da informação (dados do sensor e o sinal de controle) num NCS ou WNCS precisa ser feita usando mensagens através de uma rede. Os atrasos globais entre a amostragem do sensor e a atuação na planta podem ser variáveis porque, estes são devidos ao atraso na rede, o tempo de codificação e decodificação e atraso de transmissão da rede utilizada (com ou sem fio). Godoy et al. (2010) apresentou uma discussão detalhada sobre os componentes deste tempo de atraso na NCS. Por conseguinte, se restrições de tempo não forem cumpridas, o que significa que o tempo de espera foi afetada pelos atrasos, a execução correta do controle projetado pode ser comprometida, tornando assim o NCS mais oscilatório e até mesmo instável (BAILLIEUL et al, 2007).

Geralmente, na NCS, o *jitter* pode ser definido como uma variação de consecutivos atrasos no tempo de transmissão de mensagens na rede e pode ser medido pelo desvio padrão

do tempo de transmissão de mensagens na rede. Moyne & Tilbury (2007) afirmam que geralmente o problema de *jitter* está ligado a codificação de hardware e software (algoritmo e programação) utilizado. Investigar o *jitter* no WNCS é importante para assegurar que os atrasos de transmissão de mensagens sejam mantidos entre valores máximo e mínimo predefinidos e que esta variabilidade não vai afetar o período de tratamento e, portanto, degradar o desempenho do sistema.

De acordo com Anand et al. (2009), um elemento chave de desempenho para um WNCS é a capacidade de suportar aplicações em tempo real. Para corrigir este termo para compreender WNCS em tempo real significa que o sistema tem de ser capaz de controlar a resposta a pedidos em tempo útil, de modo que as correções tenham ainda o efeito desejado sobre a operação do processo. Resumindo, para WNCS projetar uma troca entre atrasos de tempo, perda de pacotes e *jitter* será obrigado a fornecer uma operação determinística e atingir os requisitos de controle e estabilidade. Alguns trabalhos já estão sendo realizados para comprovar a eficiência do WNCS em malhas de controle. Em Godoy et al. (2013), foram realizadas comparações entre uma malha de controle serial - ZigBee e serial – Bluetooth. Algumas dessas métricas de desempenho, tais como atraso tempo médio de transmissão ( $T_d$ ), *jitter* ( $J$ ), pior valor de atraso e mensagens perdidas foram calculados para apoiar a avaliação do dispositivo de rede sem fio mais adequada para implementar WNCS. Com base nos resultados das métricas de desempenho obtidos a partir de experiências, pode-se concluir que o dispositivo ZigBee é a melhor opção que o Bluetooth, mas ambas podem ser usadas para implementar WNCS proporcionando taxas de transmissão em malha fechada aceitáveis para várias aplicações de controle em rede.

### 3. REVISÃO CONCEITUAL

#### 3.1 PROTOCOLO MODBUS

Este protocolo define uma estrutura de mensagens compostas por bytes, que os mais diversos tipos de dispositivos são capazes de reconhecer. Embora seja utilizado normalmente sobre conexões seriais padrão RS-232, ele também pode ser usado como um protocolo da camada de aplicação de redes industriais tais como Ethernet TCP/IP. No campo das Redes Industriais, este é talvez o protocolo de mais larga utilização, já que diversos controladores e ferramentas para desenvolvimento de sistemas supervisórios utilizam este protocolo. Isto se deve a sua grande simplicidade e facilidade de implementação.

O Modbus é um protocolo aberto e uma estrutura de mensagens de comunicação usadas para transferir dados discretos e analógicos entre dispositivos microprocessados com detecção e informação de erros de transmissão. O Protocolo Modbus é baseado no modelo de comunicação mestre-escravo, onde apenas o único dispositivo mestre pode inicializar a comunicação, e os demais dispositivos escravos, respondem enviando os dados solicitados pelo mestre, ou realizam alguma ação solicitada. O dispositivo mestre pode endereçar cada dispositivo escravo da rede individualmente ou acessar a todos da rede através de mensagens em transmissão (*broadcast*).

Quando o mestre envia uma mensagem endereçada a um escravo, apenas o dispositivo endereçado retorna uma resposta (*response*) a uma mensagem (*query*) e nunca são gerados *responses* quando uma *query* for do tipo *broadcast*<sup>1</sup>. O formato das *query* definidas pelo protocolo Modbus é estabelecido da seguinte forma:

- *Address*: Tamanho de 1 byte. Número que define o endereço do dispositivo (escravo);
- *Function Code*: Tamanho de 1 byte. Define a ação a ser executada pelo escravo (ler dado, aceitar dado, reportar estado, reporte de erros);
- *Data*: Tamanho 0 a 252 bytes. Contém informações que o Escravo/Servidor deve usar para executar a ação definida pela função requisitada pelo Mestre/Cliente (endereços de memória, quantidade de itens transmitidos, tamanho do campo Data);

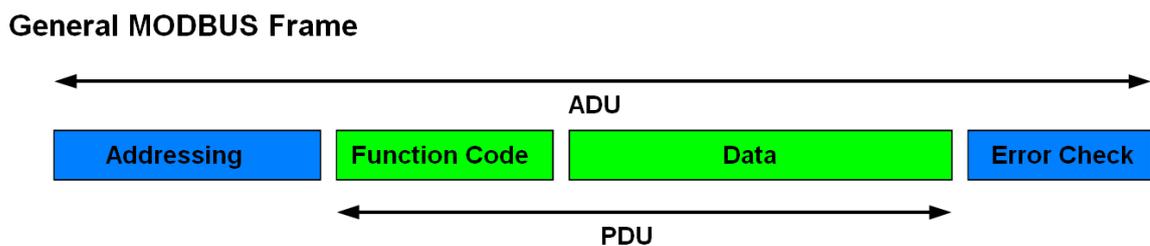
---

<sup>1</sup> Informação está sendo enviada para diversos receptores ao mesmo tempo

- *Errorcheck*: Tamanho de 2 bytes representando a checagem de erro na comunicação (enviado por um e checado pelo outro). Em caso de erro, é solicitada a retransmissão da mensagem.

A camada de aplicação Modbus define uma unidade de protocolo de dados simples, mostrada na Figura 3, independente das camadas inferiores (PDU). E o mapeamento do protocolo em portas específicas ou redes se dá por meio da unidade de aplicação de dados (ADU). O modelo mestre/escravo estabelecido pelo serviço de mensagens do Modbus é baseado em três tipos de mensagens utilizadas para a troca de informações: Modbus Request PDU (consulta), Modbus Response PDU (resposta), Modbus Exception Response PDU (erro). Neste processo o cliente envia uma mensagem de consulta (*request*), o servidor indica o recebimento e envia uma mensagem de resposta para o cliente (*response*) ou uma mensagem de erro (*exception response*).

Figura 3: Estrutura de uma Mensagem Modbus



Fonte: Modbus (2015)

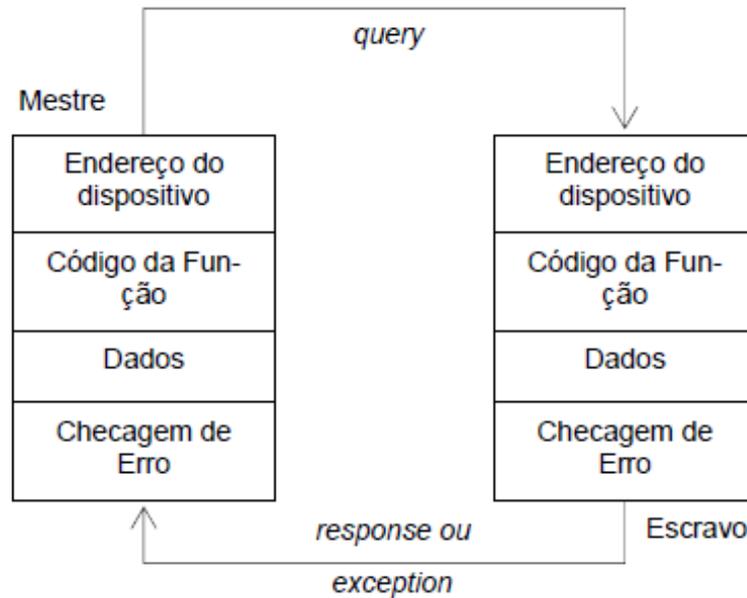
Já o formato das respostas (*response*) seguem o mesmo modelo de uma *query*, porém, são ajustadas obedecendo o formato da função requerida:

- confirmação da função;
- parâmetros pertinentes as funções;
- campo de *checksum*<sup>2</sup>.

Na existência de algum erro de comunicação, ou se o escravo não estiver apto para atender a função requisitada, o dispositivo escravo monta uma mensagem denominada *exception*, a qual justifica o não atendimento da função

<sup>2</sup> Mecanismo de verificação de erros em uma mensagem

Figura 4: Modelo de mensagem (query) Modbus



Fonte: Modbus (2015)

O protocolo Modbus pode ser configurado para trabalhar com um dos dois modos de transmissão disponíveis: ASCII (*American Standard Code for Information Interchange*) ou RTU (*Remote Terminal Unit*), os quais definem como os dados serão empacotados na mensagem, estes modos são escolhidos durante a configuração dos parâmetros de comunicação, tais como: *baud rate*, *paridade*, *stop bits*. Em uma rede industrial utilizando o protocolo Modbus, todos os dispositivos da rede devem ser configurados com o mesmo modo de transmissão.

Neste modo, cada palavra de dado da mensagem é enviada dois caracteres no padrão ASCII. A principal vantagem deste modo de transmissão é a possibilidade de haver grandes intervalos entre o envio de dados de uma mesma mensagem. O *framing*<sup>3</sup> de dados que é composto por várias palavras de dados apresentará somente valores de 30H à 39H e 41H à 46H, que correspondem respectivamente aos números de 0 à 9 e A à F no padrão hexadecimal e 0 à 9 e 10 à 15 no padrão decimal (ALFA INSTRUMENTOS, 2000).

No modo ASCII a quantidade de bits por cada palavra de dados do *framing* sempre será igual a 10, independente da configuração escolhida. Estas são as possíveis configurações:

<sup>3</sup> Pacote de dados de uma mensagem

- 1 Start bit, 7 data bits, sem paridade e 2 stop bits;
- 1 Start bit, 7 data bits, paridade PAR e 1 stop bits;
- 1 Start bit, 7 data bits, paridade IMPAR e 1 stop bits.

No campo de *checksum* é utilizado o método LRC (*Longitudinal Redundancy Check*). Um dispositivo configurado para este modo, para cada palavra de dados da mensagem é enviado apenas um caractere no padrão hexadecimal. A principal vantagem deste modo RTU em relação ao ASCII é a maior densidade de caracteres que é enviada numa mesma mensagem, aumentando o desempenho da comunicação.

Neste modo de transmissão a palavra de dados sempre será igual a 11, independente da configuração dos parâmetros.

- 1 Start bit, 8 data bits, sem paridade e 2 stop bits;
- 1 Start bit, 8 data bits, paridade PAR e 1 stop bits;
- 1 Start bit, 8 data bits, paridade IMPAR e 1 stop bits;

O campo *checksum* do *framing* é gerado pelo método CRC (*Cyclical Redundancy Check*). Nos dois modos de transmissão do protocolo Modbus, existem caracteres de identificação de início e fim de *framing*, específicos para cada modo. Com esta técnica é possível que os dispositivos escravos detectem o início de uma mensagem, identifiquem o endereço do escravo (qual escravo vai responder) ou uma mensagem *broadcast* (todos os escravos recebem, mas não respondem), e finalmente ler todo o conteúdo da mensagem até o seu final. As mensagens podem ser lidas parcialmente se ocorrer algum erro, ou existir um período maior que o *time-out*<sup>4</sup> entre o envio de uma palavra de dados e outra. Estes eventos geram as *exceptions*.

Durante a transmissão das palavras de dados neste modo, intervalos de até um segundo entre caracteres são permitidos, sem que a mensagem seja truncada (Seixas, 2009). Neste modo, o início das mensagens é identificado pelo caractere: (dois pontos), o qual corresponde ao valor ASCII 3AH. Já o término das mensagens é composto pelo conjunto de caracteres Retorno de carro (*Carriage Return - CR*) e Avanço de linha (*line feed - LF*), respectivamente com os correspondentes em ASCII aos valores 0DH e 0AH (ALFA INSTRUMENTOS, 2000).

---

<sup>4</sup> Tempo de espera de uma resposta do dispositivo antes de considerar como um erro

Os dispositivos escravos verificam constantemente o barramento e quando detectam o caractere: (3AH), se preocupam em codificar o campo seguinte que corresponde ao endereço de um dispositivo ou *broadcast*. A seguir é exibido na Figura 5 um *framing* típico no modo ASCII.

Figura 5: Framing modo ASCII

Início	Endereço	Função	Dados	LRC	Fim
: 3AH	2 caracteres	2 caracteres	N caractere	2 caracteres	CRLF

Fonte: Alfa Instrumentos (2000)

O modo RTU não possui *bytes* que identificam o início e fim da mensagem. Para identificar estes campos, não pode existir nenhuma palavra de dados por um mínimo de 3.5 vezes o tamanho da palavra de dados, esta técnica é conhecida como *silent*. Para uma taxa de 4800 bps, o tempo total de envio de uma palavra é 2291,6  $\mu$ s ( $11 \times (1/4800)$ ), ou seja, para identificar o início e fim de um *framing*, não deve ocorrer nenhuma transmissão por um período de 8,02ms ( $3,5 \times 2291,6 \mu$ s).

Neste modo, os dispositivos ficam observando os intervalos de tempo *silent* que, após detectado, dá se início ao recebimento da mensagem. No final da mensagem o mestre deve gerar outro intervalo de tempo, equivalente ao início, para caracterizar o final da mensagem.

Toda mensagem no modo RTU deve ser transmitida continuamente, pois se um intervalo de 1,5 x tamanho da palavra for detectado pelo escravo, ele descarta todos os dados que já recebeu e assume que o novo caractere que recebeu é o campo de endereço de uma nova mensagem, da mesma forma se uma mensagem for recebida em um tempo menor que o *silent* ocorrerá um erro. Abaixo é mostrado na Figura 6, um *framing* no modo RTU.

Figura 6: Framing modo RTU

Início	Endereço	Função	Dados	CRC	Fim
<i>silent</i>	1 caractere	1 caractere	N caractere	2 caracteres	<i>silent</i>

Fonte: Alfa Instrumentos (2000)

No campo de endereço de uma mensagem Modbus, podem existir dois caracteres no modo ASCII, ou 8 bits, no modo RTU. Os endereços válidos correspondem a faixa de endereço de 0 à 247, porém o endereço 0 é utilizado para *broadcast*, que é o único endereço que todos os escravos reconhecem além do próprio (ALFA INSTRUMENTOS, 2000). Quando um escravo retorna um *response* para uma máquina mestre, ele coloca seu próprio endereço na mensagem para identificá-lo.

No campo de funções também são utilizados dois caracteres no modo ASCII, ou 8 bits, no modo RTU. As funções válidas estão presentes na faixa de 1 à 255, porém nem todas estão implementadas e muitas são comuns para diversos tipos de controladores.

O dispositivo mestre deve ter a responsabilidade de verificar o campo de função das respostas dos escravos, pois este campo informa se houve problemas com a função solicitada, ou seja, se não houve nenhum problema, o escravo retorna no campo de funções o mesmo valor da função solicitada pelo mestre, mas se houve problemas o escravo devolve o mesmo valor da função, porém com o seu bit mais significativo em 1 (nível alto).

Este campo é formado por dois caracteres no modo ASCII, ou 1 *byte* no modo RTU. Ele pode variar de 00H à FFH. Neste campo existem informações relacionadas com o código da função no campo de funções, como por exemplo, o número de variáveis discretas a serem lidas ou ativadas.

Podem ocorrer os seguintes erros na transmissão de uma mensagem nos seguintes casos:

- se o escravo não recebeu a mensagem do mestre por problemas de comunicação, o escravo não retorna nenhuma mensagem, e o mestre irá verificar o timeout;
- se o escravo recebeu a mensagem, porém detectou problemas de comunicação, ele também não irá retornar uma mensagem ao mestre, e o mestre verifica o *time-out*;
- se o escravo recebeu uma mensagem sem erros de comunicação, mas ele não foi capaz de atender a solicitação, ele irá retornar ao mestre uma *exception* informando ao mestre a natureza do erro.

Abaixo na Tabela 1, alguns códigos de *exceptions* e seus significados:

Tabela 1: Exceptions

Código	Descrição
1	Função inválida
2	Registrador inválido
3	Valor de dado inválido
4	Falha no dispositivo
5	Estado de espera
6	Dispositivo ocupado
7	Não reconhecimento
8	Erro de paridade

Fonte: Modbus (2015)

Este campo é verificado ora pelo dispositivo mestre ora pelo dispositivo escravo. No modo ASCII utiliza o método LRC, e no modo RTU o CRC.

O cálculo deste campo é realizado utilizando todos os campos da mensagem exceto os caracteres de início: 3A e fim de mensagem CRLF. O valor gerado por este método é de 8 bits, e, portanto, possui dois caracteres ASCII. O LRC é calculado pelo escravo logo no recebimento da mensagem e em seguida comparado com o valor do LRC recebido. O calculado é feito a partir da adição sucessiva dos 8 bits dos campos da mensagem, descartando possíveis bits de estouro, e submetendo o resultado final a lógica de complemento de dois. Assim como o resultado tem que necessariamente ser um valor de 8 bits e o resultado das adições sucessivas provavelmente excederá 255 o valor máximo permitido, simplesmente é descartado o nono *bit*.

Na checagem do *framing* (CRC) é gerado um valor de 16 bits, onde os 8 bits menos significativos são enviados primeiros e os 8 bits mais significativos após. Este método exige uma maior complexidade para o seu desenvolvimento, porém é mais confiável.

As funções em Modbus variam de 1 a 255 (01H a FFH), mas apenas a faixa de um a 127 (01H a 7FH) é utilizada, já que o *bit* mais significativo é reservado para indicar respostas de exceção (Seixas, 2009). A maioria das funções funcionam em diversos dispositivos e outras ainda devem ser implementadas.

A leitura de entradas e saídas discretas e registradores estão descritas abaixo:

- *Read Coil Status*: leitura de saídas discretas – código 01. Formato: endereço inicial 2 bytes e número de saídas 2 bytes;
- *Read Input Status*: leitura de entradas discretas – código 02. Formato: endereço inicial 2 bytes e número de saídas 2 bytes.
- *Read Holding Registers*: leitura de registradores do dispositivo escravo – código 03. Formato: endereço inicial 2 bytes e número de registradores 2 bytes;
- *Read Input Registers*: leitura dos valores das entradas dos registros – código 04. Formato: endereço inicial 2 bytes e número de registradores 2 bytes;
- *Preset Single Register*: escrita de um valor em registrador – código 06. Formato: endereço 2 bytes e valor 2 bytes.

Atualmente, pode se encontrar aplicações para utilização do protocolo Modbus em diversas áreas. Desde o controle de motores, inversores inteligentes a controle de poços de petróleo, ou seja, a implementação deste protocolo é confiável e principalmente fácil.

O protocolo Modbus é implementado atualmente usando três versões (MODBUS, 2015):

- TCP/IP sobre Ethernet - Este modo implementa dados encapsulados em formato binário, em quadros TCP (*Transmission Control Protocol*), usando o protocolo Ethernet (IEEE 802.3). O controle de acesso ao meio utilizado é o Acesso Múltiplo por Detecção de Portadora com Detecção de Colisão (CSMA-CD);
- Transmissão Serial - Este modo opera em meio físicos variados (fios, fibra óptica e rádio). Os principais protocolos são: EIA / TIA-232-E (conhecida como RS232), EIA-422 (conhecida como RS422) e EIA / TIA-485-A (conhecida como RS485). O modo de transmissão em serial tem duas variantes: Modbus RTU - os dados são transmitidos em formato binário 8-bit e Modbus ASCII - os dados são transmitidos em formato ASCII de 7 bits;
- Modbus Plus - Este modo implementa uma rede de transferência de alta velocidade com muitos recursos adicionais para o encaminhamento, o diagnóstico, a consistência dos dados e endereçamento. Embora mais robusto e eficiente, este modo não tem uma especificação aberta, uma vez que é de domínio da Schneider Electric.

É importante citar que todas as mensagens Modbus são transmitidas no mesmo formato. A única diferença entre as três versões de protocolos está em como as mensagens são codificadas.

### 3.1.1 MODBUS TCP

Modbus TCP/IP (também Modbus-TCP) é simplesmente o protocolo Modbus RTU com uma interface TCP que funciona em Ethernet. Na estrutura de mensagens Modbus é o protocolo de aplicação que define as regras para organizar e interpretar a dados independentes do meio de transmissão de dados. TCP/IP refere-se ao protocolo e *Internet Transmission Control Protocol*, que fornece o meio de transmissão de mensagens TCP/IP Modbus.

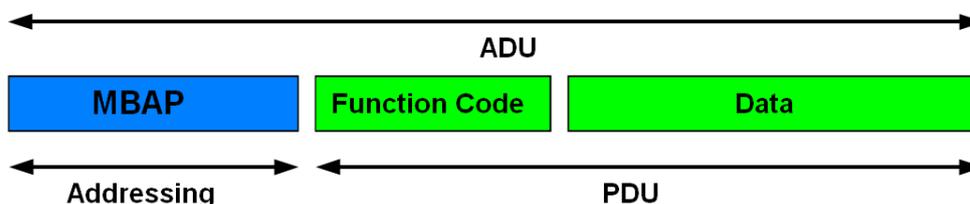
Simplificando, TCP/IP permite que blocos de dados binários possam ser trocadas entre computadores. Ele também é um padrão mundial que serve como base para a *World Wide Web*. A função primária de TCP é de assegurar que todos os pacotes de dados serão recebidos corretamente, enquanto o IP que garante que as mensagens sejam dirigidas corretamente e encaminhadas. Note-se que a combinação de TCP/IP é apenas um protocolo de transporte, e não define o que os dados significa ou como os dados devem ser interpretados (este é o trabalho do protocolo de aplicação, Modbus, neste caso).

Então, em resumo, Modbus TCP/IP utiliza o TCP/IP e Ethernet para transportar os dados da estrutura da mensagem Modbus entre dispositivos compatíveis. Isto é, TCP/IP Modbus combina uma rede física (Ethernet), com um padrão de rede (TCP/IP), e um método padrão de representação de dados (Modbus como o protocolo da aplicação). Essencialmente, a mensagem TCP/IP Modbus é simplesmente uma comunicação Modbus encapsulado em um invólucro de TCP/IP Ethernet.

Na prática, Modbus TCP incorpora um *frame* de dados Modbus padrão em um *frame* TCP, sem a soma de verificação Modbus. Os comandos Modbus e dados do utilizador são encapsulados no interior do recipiente de dados de uma mensagem TCP/IP sem modificar a estrutura básica da mensagem Modbus. As diferenças estão na interpretação do endereço (IP) e na verificação de erro (CRC-32) conforme mostrado na Figura 7.

Figura 7: Estrutura de uma Mensagem Modbus TCP/IP

### MODBUS/TCP Frame



Fonte: Modbus (2015)

No entanto, o campo de verificação de erro Modbus (*checksum*) não é usado como os métodos da camada de enlace de soma de verificação TCP/IP Ethernet padrão, em vez disso são usados para a garantia de integridade dos dados. Além disso, o campo de endereço do *frame* Modbus é suplantado pelo identificador de unidade no Modbus TCP/IP, e torna-se parte do cabeçalho *Modbus Application Protocol* (MBAP).

Os campos de código de função e dados são absorvidos em sua forma original. Assim, uma unidade de dados de aplicativos TCP/IP Modbus (ADU) assume a forma de um cabeçalho de 7 byte (identificador de transação + identificador de protocolo + campo de comprimento + identificador da unidade), e a unidade de dados de protocolo (código de função de dados). O cabeçalho MBAP é de 7 bytes de comprimento e inclui os seguintes campos:

- Identificador de Transação / invocação (2 Bytes): Este campo de identificação é usado para emparelhamento da transação quando várias mensagens são enviadas ao longo da mesma conexão TCP por um cliente sem esperar por uma resposta antes.
- Protocolo *Identifier* (2 bytes): Este campo é sempre 0 para serviços Modbus e outros valores são reservados para futuras extensões.
- Comprimento (2 bytes): Este campo é uma contagem de bytes dos campos restantes e inclui o byte unidade identificador, byte código de função, e os campos de dados.
- Unidade Identificador (1 byte): Este campo é usado para identificar um servidor remoto localizado sobre uma rede sem TCP/IP.

Em um aplicativo de servidor Modbus TCP/IP típica, a ID da unidade está definida para 00 ou FF, ignorado pelo servidor, e simplesmente ecoou de volta na resposta. O Modbus TCP/IP ADU completo é incorporado em um campo de dados no padrão TCP e enviados para a porta

502, que é reservado especificamente para aplicações Modbus. Podemos ver que a operação do Modbus sobre Ethernet é quase transparente para a estrutura registrador/comando.

A Ethernet IEEE 802.3 é um protocolo de rede de escritório que ganhou aceitação em todo o mundo. Ele também é um padrão aberto que é suportado por muitos fabricantes e sua infraestrutura está amplamente disponível e instalado. Como muitos dispositivos já suportam Ethernet, seria fácil sua ampliação para uso em aplicações industriais.

Tal como aconteceu com a Ethernet, o Modbus está disponível, acessível a qualquer um, e amplamente apoiada por muitos fabricantes de equipamentos industriais. Também é fácil de compreender que se torna um candidato natural para utilização na construção de outros padrões de comunicação industrial. Com tanta coisa em comum, a junção do protocolo de aplicação Modbus com transmissão Ethernet IEEE 802.3 tradicional constitui um poderoso padrão de comunicação industrial em Modbus TCP/IP. E porque Modbus TCP/IP compartilha as mesmas camadas física e de enlace de dados de tradicional IEEE 802.3 Ethernet e usa o mesmo suíte de protocolos TCP/IP, continua a ser compatível com a infraestrutura de cabos Ethernet já instalado, conectores, placas de rede, hubs e switches.

### 3.1.2 MODBUS WI-FI – WI-FI 802.11

Redes locais sem fio (WLAN) podem operar em 2,4 GHz ou 5 GHz. Estas redes suportam dois modos: *ad-hoc* e de infraestrutura. O modo *ad-hoc* permite que todas as estações se comuniquem uns com os outros de forma *peer-to-peer*. O modo de infraestrutura, a rede tem um ponto de acesso (AP), por meio do qual, cada estação cliente se comunica.

Em automação de processos, as redes Wi-Fi podem servir como a espinha dorsal para a concentração de dados. Por exemplo, ele pode ser usado em conjunto com uma rede de curto alcance, dispositivos de campo de baixa potência em uma rede sem fio para coletar dados a partir do *gateway* de enviá-lo para a sala de controle ou outro ponto de coleta de dados.

As vantagens de WLAN em automação de processos incluem: padrões abertos, robustez, boa relação custo-benefício, fácil acessibilidade e alta taxa de transmissão de dados (Emerson Process, 2006). A segurança também aumentou com duas melhorias de segurança, Wi-Fi *Protected Access* (WPA) e WPA2, que substituem tecnologia mais antiga e menos segura.

Além disso, usado em conjunção com, por exemplo, uma rede de sensores sem fios, que oferecem largura de banda suficiente para suportar múltiplos meios. No entanto, WLAN pode não ser aplicável para comunicação sem fio para dispositivo por causa do alto consumo de

energia, exigindo a alimentação da linha ou *Power over Ethernet* (PoE). As despesas de proporcionar as linhas de alimentação podem limitar o tamanho da rede (Emerson, 2006b). Além disso, é projetada mais para aplicações de rendimento elevados para pequeno número de terminais (DZUNG et al., 2005), que é bastante oposto a algumas características WNCS.

O protocolo Wi-Fi IEEE 802.11 possui ainda uma característica importante entre os dispositivos sem fio que deve ser considerado quando o controle é implementado através de uma WLAN. Embora o protocolo IEEE 802.11, não tenha sido concebido para aplicações em WNCS, a sua implementação pode ser útil no controle de rede quando define o DCF (*Distributed Control Function*). Neste protocolo, a decisão da estação que pode transmitir é tomada entre os nós da WLAN (MILLAN et al., 2011).

A especificação da família do protocolo 802.11 foi concebido como um método para ampliar o acesso sem fio à infraestrutura Ethernet, entre eles está:

- IEEE 802.11b é uma velocidade baixa para as extensões de protocolo mais recentes. Ele usa um algoritmo de introduzir código cortesia para uma taxa de dados máxima de 11 Mbps. Levando-se em conta cabeçalhos de mensagens, espaçamento entre e outros encargos gerais, a taxa máxima de dados prático é cerca de 7 Mbit/s. Quando os dados são divididos em pacotes de menores, no entanto, esta transferência pode ser ainda mais baixa, por exemplo, de 0,75 Mbps para cargas úteis de 60 bytes de dados (PIGGIN et al, 2006). Esta diminuição da taxa de transferência é de particular relevância para uma aplicação de controle onde os pacotes de dados são raramente mais de uma centena Bytes. IEEE 802.11b ocupa cerca de largura de banda de 25MHz na banda ISM entre 2402 e 2482 MHz, permitindo até três canais coexistindo não sobrepostos.
- IEEE 802.11g é uma extensão de alta velocidade que é totalmente compatível com 802.11b. Ele também suporta um *Orthogonal Frequency Division Multiplexed* (OFDM) multiplexadora na camada física que é capaz de uma modulação 54 Mbps. A taxa de dados com uma carga útil de 60 bytes é limitada a 2 Mbps (PIGGIN et al, 2006). O IEEE 802.11g também ocupa a banda ISM e ocupa uma 25MHz de largura de canal fixo, assim, permitindo também três canais coexistentes.
- IEEE 802.11a usa o PHY OFDM, mas é colocado na banda U-NII cobrindo 5,15 GHz a 5,35 GHz e 5.725 GHz a 5.825 GHz. Este loteamento de faixa mais larga abre espaço para 9 transmissões não sobrepostas paralelas, e com os 54 Mbps esquema de codificação de uma taxa de prática de cerca de 30 Mbps é plausível. Mais uma vez com as cargas de dados menores esperados em aplicações de controle, as taxas de dados são

reduzidas significativamente para cerca de 2,6 Mbps para os pacotes de 60 bytes (PIGGIN et al, 2006).

O formato da estrutura (*frame*) para uma transmissão 802.11 inclui grandes despesas gerais (tão elevadas como 64 bytes) na forma de um preâmbulo, MAC cabeçalho e sufixo CRC. Assim, em todas as variantes da especificação 802.11, tamanhos menores de dados resultam em baixo rendimento. Em aplicações de controle, reconhecimentos na camada de aplicação são por vezes incluídos para garantir a entrega dos dados. Escolhendo o TCP/IP ou um protocolo de transmissão equivalente reconhecido, reduz a taxa de transferência eficaz por adicionar mais sobrecarga para as mensagens de confirmação, espaços entre frame, etc. Na Tabela 2 podemos ver as principais diferenças entre os protocolos sem fio.

Tabela 2: Parâmetros para protocolos sem fio

Parâmetro	802.11a	802.11b	802.11g
Faixa de Frequência	5 GHz	2,4 GHz	2,4 GHz
Potência	20 dBm	20 dBm	20 dBm
Max. Taxa de dados	54 Mbps	11 Mbps	54 Mbps
Taxa de dados – 60Byte	3,9 Mbps	1,7 Mbps	4.4 Mbps

Fonte: Piggín & Brandt (2006)

A implementação de uma célula sem fio WiFi poderia ser *ad-hoc* ou auto-organização; no entanto a maioria dos aplicativos usar um ponto de acesso centralizado a execução de uma função de coordenação entre os vários nós clientes conectados a ele.

### 3.2 DETERMINISMO

Determinismo é um termo que é utilizado aqui para descrever a capacidade do protocolo de comunicação em garantia de que uma mensagem é enviada ou recebida em uma quantidade finita e de tempo previsível. Podemos supor que, para aplicações de controle críticos, o determinismo é muito importante.

Historicamente, a Ethernet tradicional não foi considerado um barramento de campo viável para redes de entradas e saídas por causa de duas grandes deficiências de controle industrial, a inerente não-determinismo, e baixa durabilidade. No entanto, as novas tecnologias aplicadas corretamente têm resolvido a maioria destas questões.

Originalmente, o equipamento Ethernet foi projetado para o ambiente de escritório, ambientes industriais não agressivos. Embora, muitas instalações Ethernet em fábricas possam usar este hardware padrão sem problemas, novos conectores classificados com industriais, cabos blindados e switches e hubs mais robustos, estão agora disponíveis para ajudar a resolver o problema da durabilidade.

No que diz respeito ao comportamento não determinístico da Ethernet, este é em grande parte um resultado da arbitragem de acesso do protocolo que é usada para a transmissão na rede. Ou seja, *Carrier Sense Multiple Access com Collision Detect* (CSMA/CD). Uma vez que qualquer dispositivo de rede pode tentar enviar um pacote de dados em qualquer momento, com CSMA/CD aplicada, cada dispositivo irá primeiro verificar se a linha está livre e disponível para utilização. Se a linha estiver disponível, o dispositivo começará a transmitir o seu primeiro frame. Se um outro dispositivo também tenta enviar um frame aproximadamente ao mesmo tempo, em seguida, ocorre uma colisão e ambos os frames serão descartados. Cada dispositivo, em seguida, espera uma quantidade aleatória de tempo e repete a sua transmissão até que seu frame seja enviado com êxito. Este método de alocação de canais é intrinsecamente não-determinístico porque um dispositivo só pode transmitir quando a rede está livre, resultando em tempos de espera imprevisíveis antes que os dados possam ser transmitidos.

Como a maioria dos sistemas de controle têm uma exigência de tempo definido para a transmissão de pacotes, normalmente menos de 100ms, o potencial para colisões e o método CSMA/CD de retransmissão não é considerado um comportamento determinística e esta é a razão que a Ethernet tradicional tem tido problemas para ser aceito para uso em aplicações de controle crítico. No entanto, CSMA/CD é naturalmente suprimida em uma rede de dispositivos que estão interligados através de switches Ethernet. Esta composição é comumente referida como a Ethernet comutada em um esforço para distinguir-se do comportamento não-determinística da Ethernet tradicional.

Ethernet é feita mais determinística através da utilização de chaveadores rápidos de Ethernet (*Switches Fast Ethernet*) para interligar dispositivos. Estes *switches* aumentam a largura de banda de grandes redes subdividindo-os em várias redes menores ou "domínios de colisão" separadas. O *switch* também minimiza o *jitter* da rede, facilitando uma ligação direta a partir de um emissor para um receptor, de tal maneira que apenas o receptor recebe os dados, não a totalidade da rede. Cada porta de um *switch* encaminha os dados para outra porta com base no endereço MAC contido no pacote de dados/frame recebido. O *switch* armazena os endereços MAC de cada aparelho que está conectado juntamente com o número da porta associada. Desta forma, o domínio de colisão Ethernet para na porta do *switch*, e o *switch* quebra

eficazmente a rede separada em ligações de dados ou domínios de colisão em cada porta distinta do *switch*. A capacidade do *switch* para direcionar um pacote para uma porta específica, em vez de encaminhá-lo a todas as portas de *switch*, também ajuda a eliminar as colisões que fazem a Ethernet não-determinística.

Então, como os *switches* tornaram-se mais baratos, a tendência atual em aplicações críticas de controle industrial é conectar um dispositivo Ethernet em cada porta do *switch*, tratar eficazmente o dispositivo de comutação como o centro de uma rede em estrela. Uma vez que existe apenas um dispositivo ligado a uma porta, não há nenhuma possibilidade de ocorrer colisões. Isso suprime eficazmente a rotina CSMA/CD. Desta forma, com apenas um dispositivo de rede conectado por porta do *switch*, o *switch* pode executar uma transmissão nos dois sentidos (*full-duplex*), sem chances de colisões. Assim, um *switch* Ethernet 10/100 é executado de forma eficaz a 20/200 Mbps, pois pode transmitir e receber a 10 ou 100 Mbps simultaneamente nos dois sentidos. A velocidade de transferência mais elevada de *full-duplex* acoplado sem a necessidade de invocar CSMA/CD produz um modo mais determinística de operação, ajudando aplicações de controle crítico para permanecer previsível.

Os *switches* não podem filtrar completamente o tráfego transmitido em rede de uma empresa, e isso pode causar colisões adicionais reduzindo o determinismo de uma rede conectando mais de um dispositivo a uma porta do *switch*. No entanto, se a rede da empresa e a rede de controle industrial podem ser separadas, nenhum tráfego é adicionado à rede de controle e o seu determinismo é aumentado. Além disso, se um *switch* é usado para separar as duas redes, este *switch* pode ser geralmente configurado para filtrar o tráfego desnecessário.

Assim, podemos combinar um projeto de rede com *switch* quando é necessário aumentar o determinismo de uma rede, tornando a rede Ethernet mais atraente. Outros avanços em *switches* Ethernet, tais como, velocidades mais altas, proteção contra tempestades de transmissão, suporte a rede virtual local (VLAN), protocolo de gerenciamento de redes (SNMP), e prioridade de mensagens de ajuda adicional podem aumentar o determinismo das redes Ethernet. Como a velocidade de 10 Gbps na Ethernet entrando no mercado, o determinismo não será mais uma preocupação.

## 4. MATERIAIS E MÉTODOS

Baseando-se nas necessidades e oportunidades citadas, este trabalho, de forte cunho experimental, objetiva o projeto e implementação de uma plataforma experimental de WNCS com equipamentos industriais, a qual será usada para analisar o desempenho de controladores PID aplicados em WNCS industriais.

### 4.1 IMPLEMENTAÇÕES DO MODBUS

Modbus é um protocolo de comunicação da camada de aplicação, representada pela camada sete do modelo OSI<sup>5</sup> e, portanto, independente das outras seis camadas, sendo apenas necessário que elas sejam funcionais. No caso de redes wireless como pode ser visto na Figura 8. Isso permite vários métodos de implementar o uso do Modbus com diferentes meios físicos.

Figura 8: Implementação do Modbus WiFi

Modelo ISO/OSI de Camadas		Modbus TCP/IP ou WiFi	Implementação
7	Aplicação	Modbus	Arduino
6	Apresentação		
5	Sessão		
4	Transporte	Protocolo TCP	Pilha TCP/IP
3	Rede	Protocolo IP	
2	Enlace		Ethernet Shield ou Módulo XBee Wi-Fi
1	Física	Ethernet ou Wi-Fi	

Fonte: Autoria própria

Neste trabalho, foram implementadas uma versão do Modbus TCP/IP e do Modbus WiFi, baseadas em Arduino, para uso em aplicações de controle via rede sem fio baseadas em Modbus. A camada de aplicação do Modbus foi implementada em código na plataforma Arduino. Através do uso de uma pilha TCP/IP compatível, juntamente com um módulo *shield* Ethernet para Arduino ou um módulo XBee WiFi como pode ser visto na Figura 9 é possível realizar a comunicação de dados via Modbus TCP/IP ou Modbus WiFi.

<sup>5</sup> Modelo para a arquitetura de um protocolo de comunicação de dados

Figura 9: Conjunto do Arduino com shield XBee e Ethernet

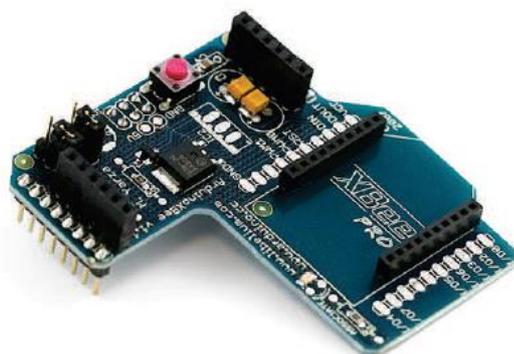


Fonte: <http://www.filipeflop.com/pd-6b60d-xbee-shield-para-arduino.html>

O Arduino é uma plataforma de código aberto (*open-source*) de prototipagem de hardware baseada em uma simples placa de microcontrolador e uma interface de desenvolvimento de software. Seu objetivo é tornar o desenvolvimento de projetos de eletrônica mais acessíveis, fornecendo uma interface e bibliotecas amigáveis ao usuário. O hardware consiste em uma placa com I/Os disponíveis para uso imediato, permitindo o acesso simplificado a todas as funcionalidades disponibilizadas pelo microcontrolador utilizado.

O software consiste em um ambiente de desenvolvimento integrado (IDE) com compilador para código em C e de um software de carregamento (*bootloader*) para o microcontrolador, permitindo a gravação serial diretamente a partir de uma porta serial virtual. Por suas qualidades o Arduino atraiu diversos desenvolvedores não só de hardware, mas de software também, e hoje temos disponíveis uma enorme quantidade de bibliotecas para Arduino que facilitam enormemente qualquer tipo de desenvolvimento. Ela também é compatível com anteparos (*shields*) XBee disponíveis, como vemos na Figura 10.

Figura 10: Shield XBee

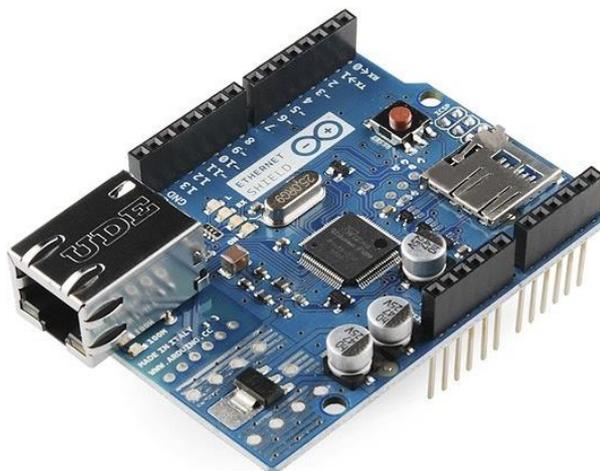


Fonte: <http://www.filipeflop.com/pd-6b60d-xbee-shield-para-arduino.html>

As placas que podem ser encaixadas em cima de uma placa Arduino são chamadas de *Shields*, estendendo assim suas funcionalidades. Os *shields* seguem a mesma filosofia que as placas do Arduino, sendo fáceis de montar, baratos e *open-hardware*. Neste trabalho foram usados *shields* XBee e Ethernet para facilitar a interface do Arduino com os módulos evitando a necessidade do uso de mais circuitos periféricos.

O *Shield* de Ethernet permite a conexão da placa Arduino à Internet. Baseia-se no chip Wiznet W5500 Ethernet. Ele suporta até oito conexões de soquete simultâneos. O *shield* Ethernet da Figura 11, conecta a uma placa Arduino usando longas conexões que se estendem através da *shield*. Isso mantém a aparência de pino intacto e permite que outro *shield* seja empilhada em cima dela. Há um slot para cartão micro-SD integrado, que pode armazenar arquivos para serem usados através da rede. Possui também uma conexão padrão RJ-45, com um transformador de linha.

Figura 11: Shield Ethernet



Fonte: <http://www.filipeflop.com/pd-6b60d-xbee-shield-para-arduino.html>

XBee é o nome dado a uma família de módulos de radiofrequência desenvolvidos e distribuídos pela *Digi International* como mostrado na Figura 12.

Figura 12: XBee WiFi



Fonte: <http://www.filipeflop.com/pd-6b60d-xbee-shield-para-arduino.html>

Esta família tem como características implementar módulos de radiofrequência de baixo custo e baixo consumo para aplicações especificadas pelo protocolo IEEE 802.11 ou WiFi. O XBee Wi-Fi combina hardware com software para uma solução modular completa e apresenta as seguintes vantagens:

- dispositivo de integração em nuvem nativo para aquisição de dados e gerenciamento de dispositivos,
- módulo de hardware e software completo e de fácil junção a infraestrutura existente (WiFi802.11 b/g/n),
- a disposição física (pinagem) comum do XBee permite que fabricantes originais dos equipamentos (OEM) possam suportar uma variedade de protocolos sem fio,
- suporte a comunicação serial do tipo SPI<sup>6</sup> e UART<sup>7</sup>;
- suporte para aplicações sleep (sono) de baixa potência com corrente de desligamento menor que 6 mA,
- taxas de dados de até 72 Mbps,
- métodos de provisionamento simples incluindo *Soft AP* e *Wi-Fi Protected Setup (WPS)*.

---

<sup>6</sup> Serial Peripheral Interface é um protocolo que permite a comunicação serial síncrona do tipo mestre-escravo entre componentes, principalmente em sistemas embarcados.

<sup>7</sup> Universal Asynchronous Receiver/Transmitter é utilizado para comunicação serial assíncrona entre componentes.

O módulo XBee Wi-Fi é compatível pino a pino com toda a família de módulos XBee fornecidos por essa empresa. Permite a troca de dados entre dispositivos da rede via endereçamento IP. Com o módulo XBee Wi-Fi, é possível se comunicar com dois tipos de redes IEEE 802.11 b/g/n, infraestrutura e Ad-Hoc.

Na rede tipo Infraestrutura é necessário a existência de um Access Point (AP), onde é possível conectar vários XBee Wi-Fi. Já numa rede Ad-Hoc não se utiliza Access Point. Para criar uma rede Ad-Hoc é preciso somente de um computador com adaptador Wi-Fi e um módulo XBee Wi-Fi configurado no modo IBSS (Independent Basic Service Set - Conjunto de Serviços Básicos Independentes). Nessa mesma configuração, é possível criar uma rede ponto a ponto de módulos XBee Wi-Fi, configurando um módulo como criador da Rede (IBSS CREATOR) e os demais módulos como (IBSS JOINER), que poderão aderir a uma rede existente.

O módulo Wi-Fi pode ser configurado para trabalhar no modo transparente (comandos AT) ou no modo API (modo avançado), onde é possível enviar quadros de dados no padrão IEEE 802.15.4 ou no padrão IPV4. No modo API, o XBee Wi-Fi permite enviar e receber quadros no mesmo formato dos módulos XBee S1 (IEEE 802.15.4), mas a comunicação Wi-Fi com esses módulos não é possível, pois ambos utilizam protocolos diferentes. Módulos XBee Wi-Fi só se comunicam com dispositivos que tenham a mesma especificação, a IEEE 802.11 b/g/n.

O módulo XBee Wi-Fi foi configurado para trabalhar da seguinte forma:

- protocolos IP: UDP ou TCP,
- modo de endereçamento: DHCP ou STATIC,
- encriptação: WPA (TKIP), WPA2 (AES) e WEP,
- interfaces Seriais: USART (1200 bps a 1 Mbps) e SPI (até 3,5 Mbps).

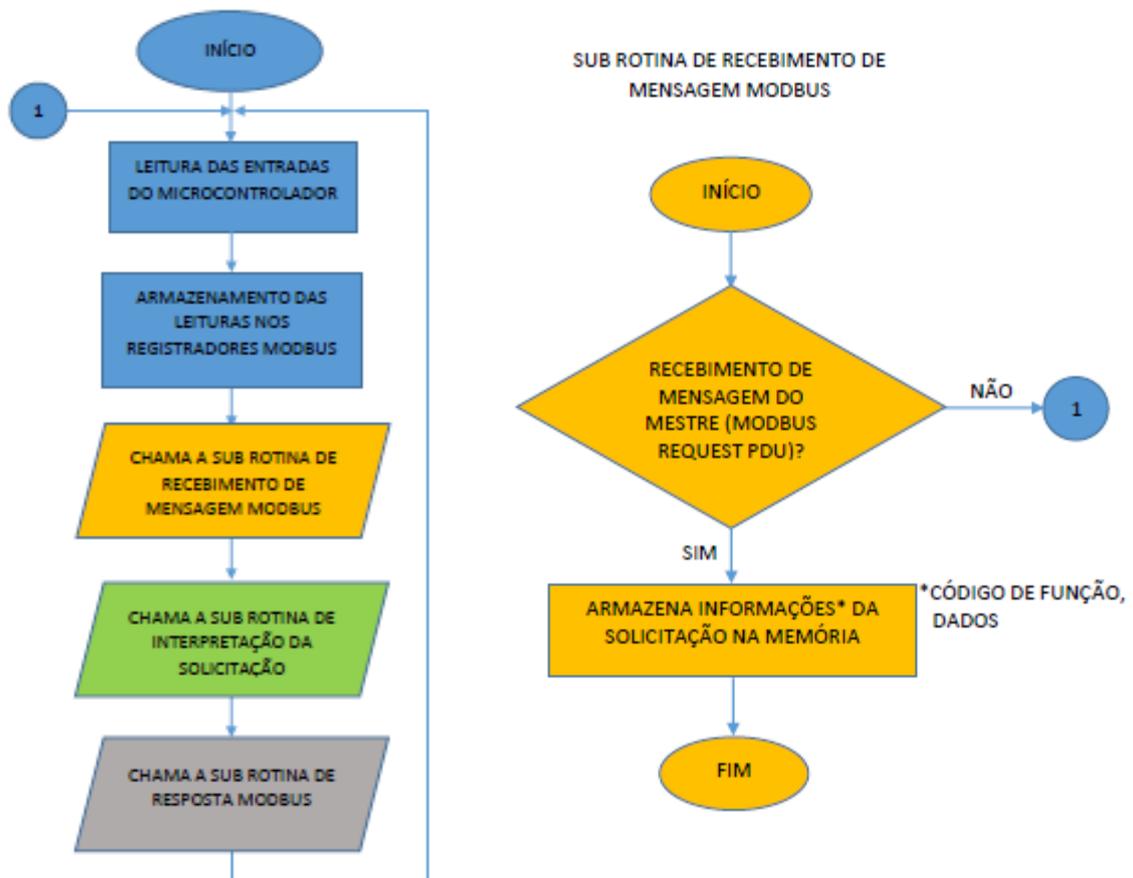
Através da integração dos equipamentos citados, é possível a comunicação com e sem fio utilizando os protocolos de comunicação Modbus e TCP/IP. Os protocolos TCP/IP são usados em conjunto e são os protocolos das camadas de Transporte e de Rede para uma comunicação via Ethernet. No protocolo Modbus TCP, os dados do frame Modbus são transmitidos através do protocolo TCP, juntamente com um endereço IP, de acordo com o modelo Cliente/Servidor de comunicação.

O protocolo TCP deve estabelecer uma conexão antes de transferir os dados, uma vez que é um protocolo baseado em conexão ponto a ponto. O Mestre/Cliente Modbus estabelece uma conexão com o Escravo/Servidor. O Servidor aguarda por uma conexão de entrada do Cliente, e estabelecida a conexão, responde às consultas ou requisições de dados até que a conexão seja encerrada.

Conforme descrito, neste trabalho a implementação do Modbus TCP/IP foi realizada utilizando um microcontrolador Arduino juntamente com um Ethernet Shield ou com um transmissor sem fio Wi-Fi (*XBee S6B*). Este conjunto representa o Servidor Modbus, o qual é parametrizado com um endereço IP (ex: 192.168.1.100 para o sensor da malha) e porta 502, que é reservada para aplicações do protocolo Modbus. O Servidor não tem uma identificação, sendo que todo endereçamento da comunicação é baseado no endereço IP.

O código implementado no microcontrolador Arduino (Sketch) para implementação e comunicação via protocolo Modbus é apresentado e detalhado no fluxograma da Figura 13

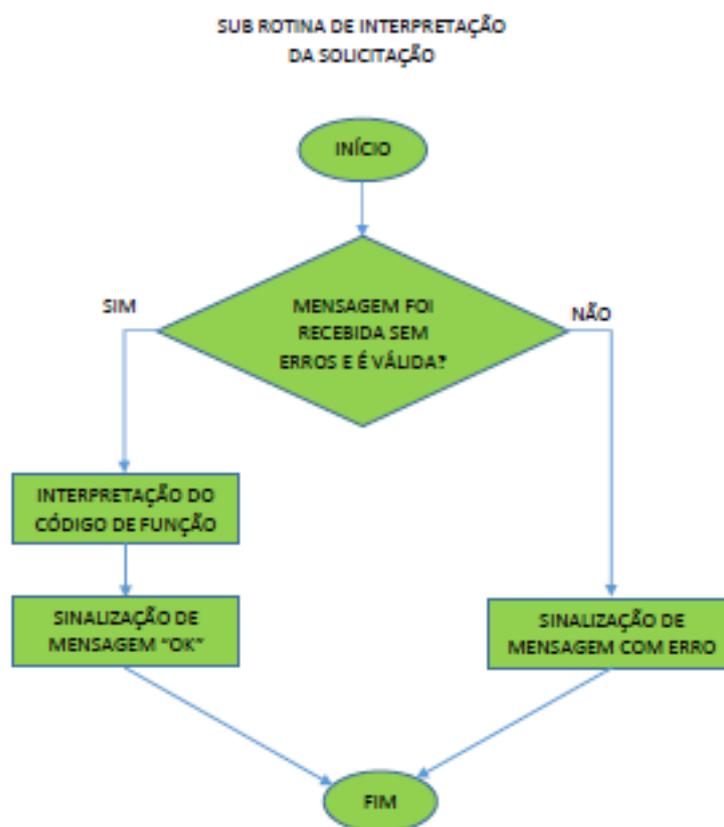
Figura 13: Fluxograma da rotina principal e da sub-rotina de recebimento de mensagens Modbus



Fonte: Autoria própria

Conforme mostrado na Figura 13, a rotina/programa principal (cor azul) é responsável por fazer a leitura das entradas de sensores conectados ao Arduino, armazenamento dessas informações nos registradores do mapa de memória Modbus do dispositivo e também é composta por três sub-rotinas com funções específicas. A sub-rotina de recebimento de mensagens Modbus (cor amarela) é responsável pela verificação do recebimento de mensagem de solicitação do Mestre/Cliente (*Modbus Request PDU*) e pelo armazenamento das informações (Código de função Modbus e Dados de interesse). Ao receber a solicitação de informação do Mestre/Cliente da rede (controlador da malha de controle em LabVIEW), o XBee irá repassar a solicitação ao Arduino de forma serial no protocolo Modbus. A solicitação do Mestre/Cliente Modbus é salva numa matriz do Arduino para interpretação de cada byte da mensagem. De acordo com a Figura 14, a sub-rotina de interpretação da solicitação Modbus verifica se a mensagem foi recebida sem erros e é válida. Em caso positivo, uma variável de sinalização é setada e através do código de função Modbus recebido (código 04: relativo à solicitação de leitura de registrador analógico de 16bits), é possível responder ao Mestre/Cliente com a informação requerida (entrada analógica que está ligada ao pino 13 do Arduino) armazenada no registrador solicitado (registrador 40010).

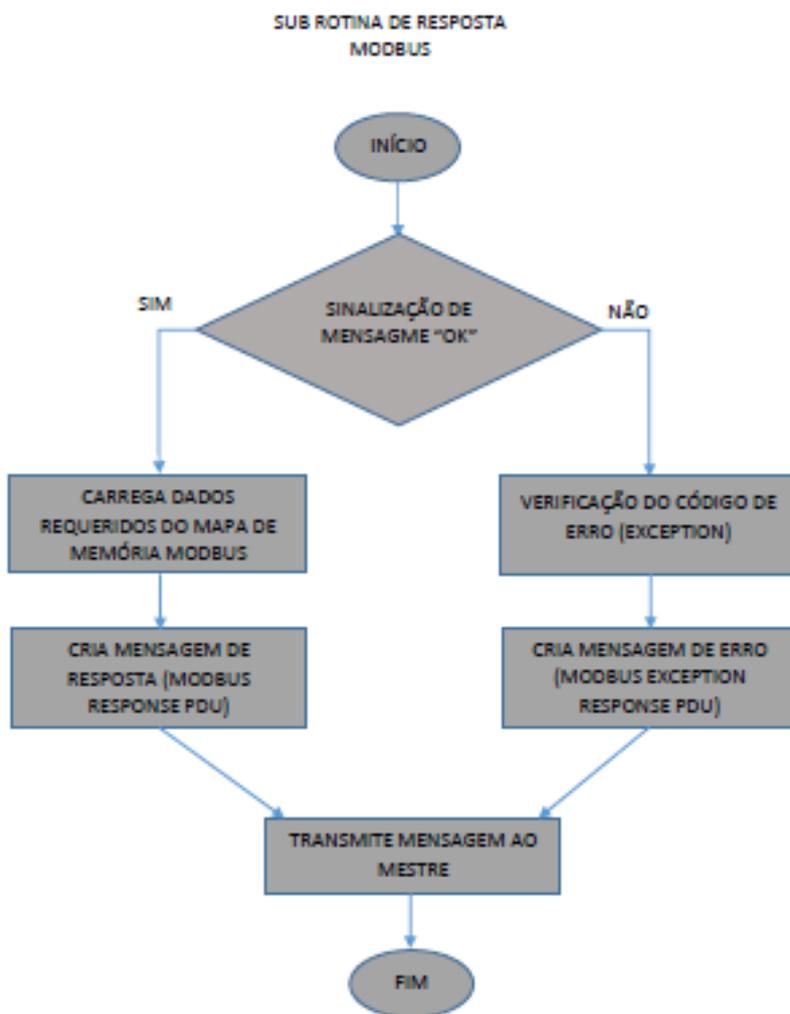
Figura 14: Fluxograma da sub-rotina de interpretação da solicitação Modbus



Fonte: Autoria própria

Essa mensagem de resposta é enviada ao Mestre/Cliente através de um frame Modbus de resposta, conforme mostrado no fluxograma da sub-rotina de resposta Modbus da Figura 15. Essa sub-rotina é responsável por verificar a variável de sinalização de mensagem Ok ou Com Erro e enviar mensagem de resposta. Caso a mensagem seja Ok (ou livre de erros), o frame Modbus (*Modbus Response PDU*) é montado repetindo as informações de endereço do Servidor/Escravo, o código da função e endereço do dado. Caso a mensagem seja Com Erro, o frame Modbus (*Modbus Exception Response PDU*) contendo a informação do erro é montado. O Arduino transmite via serial o frame Modbus montado para o Ethernet Shield ou XBee Wi-Fi, que realiza a transmissão da informação via Modbus TCP/IP (com ou sem fio) ao Mestre/Cliente finalizando o fluxograma da sub-rotina da Figura 15 e reiniciando o fluxograma da rotina principal da Figura 13.

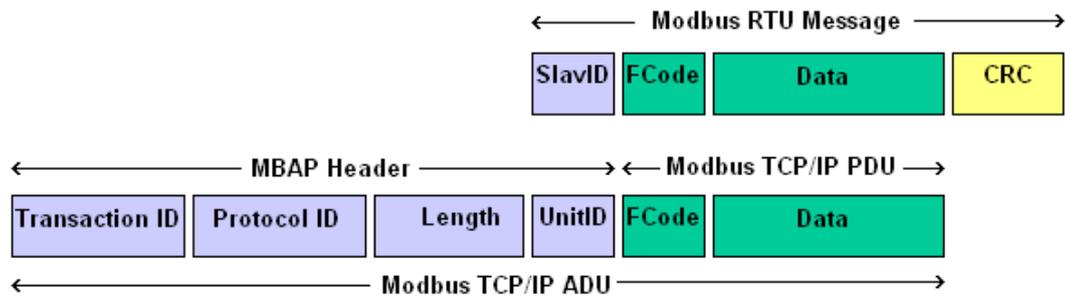
Figura 15: Fluxograma da sub-rotina de resposta Modbus



Fonte: Autoria própria

É importante verificar que existem diferenças no conteúdo da mensagem Modbus serial (RTU) e a Modbus TCP, conforme apresentado na Figura 16 essa lógica de montagem e interpretação dos frames Modbus para viabilizar a comunicação é realizada pelo Arduino.

Figura 16: Diferença entre mensagem Modbus RTU e Modbus TCP/IP



Fonte: Modbus (2015)

Para facilitar o entendimento, considere uma mensagem de um Mestre Modbus RTU, mostrada na Figura 17, solicitando o conteúdo de um registrador de entrada analógica (40108) de um dispositivo Escravo Modbus com o endereço 17. Na Figura 16, temos: 11 - endereço do servidor (17 = 11 hex), 04 - código de função Modbus (leitura de registrador de entrada analógica), 006B - endereço de dados do registrador solicitado (40108- 40001 do registrador inicial = 107 = 6B hex), 0001 - número de registradores solicitados (ler 1 registrador 40108) e B298 – verificação de erros por CRC.

Figura 17: Mensagem Modbus RTU

<b>11</b>	<b>04</b>	<b>006B</b>	<b>0001</b>	<b>B298</b>
-----------	-----------	-------------	-------------	-------------

Fonte: Autoria própria

Para o Modbus TCP, um novo cabeçalho de 7 bytes chamado cabeçalho MBAP (explicado na seção 3.1.1) é adicionado ao início da mensagem. Dessa forma, a solicitação do Mestre Modbus RTU anterior alterada para uma solicitação do Cliente Modbus TCP teria o formato mostrado na Figura 18. Na Figura 18 temos: 0001 - identificador de transação, 0000 - identificador de protocolo, 0006 - comprimento da mensagem (6 bytes), 11 - identificador da

unidade (17 = 11 hex), 04 - código de função, 006B - endereço de dados do registrador solicitado (40108), 01 - número total de registradores solicitados.

Figura 18: Mensagem Modbus TCP

<b>0001</b>	<b>0000</b>	<b>0006</b>	<b>11</b>	<b>04</b>	<b>006B</b>	<b>01</b>
-------------	-------------	-------------	-----------	-----------	-------------	-----------

Fonte: Autoria própria

#### 4.2 BANCADA DE WNCS

A implementação do sistema de controle via rede sem fio (WNCS) em estudo, foi baseada em uma Planta Piloto de Instrumentação da escola SENAI de Lençóis Paulista mostrada na Figura 19.

Figura 19: Planta Piloto de Processos – SENAI Lençóis Paulista



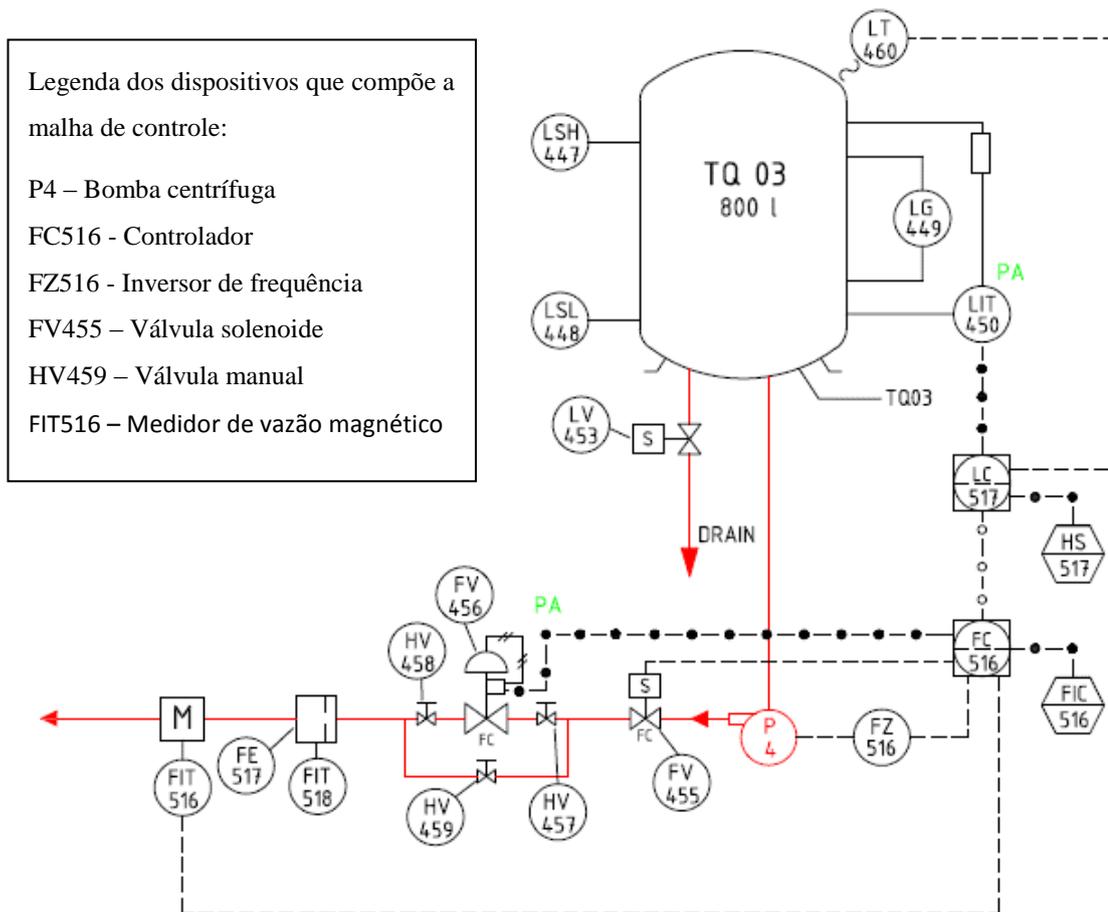
Fonte: Autoria própria

O objetivo desta planta é realizar estudos sobre instrumentos, processos e estratégias de controle, monitorando seu comportamento através de interface homem máquina implantado.

Com os dados coletados, é possível analisar a eficiência do controle da variável por meio da programação do controlador.

Para uma melhor compreensão do processo, na Figura 20 tem-se o diagrama P&ID do processo estudado, onde utilizou-se a bomba P4 ligada a um inversor de frequência como elemento final de controle e o medidor de vazão magnético FIT 516 para medir a variável a ser controlada na malha de controle.

Figura 20: Diagrama P&ID do processo em estudo



Fonte: Autoria própria

Esta planta contempla quatro CLPs de fabricantes diferentes e diversas variáveis de processo que utilizam os mais variados princípios de medição, com os principais protocolos de comunicação em rede industrial, conforme apresentado apresentados na Tabela 3.

Tabela 3: Recursos disponíveis na planta piloto

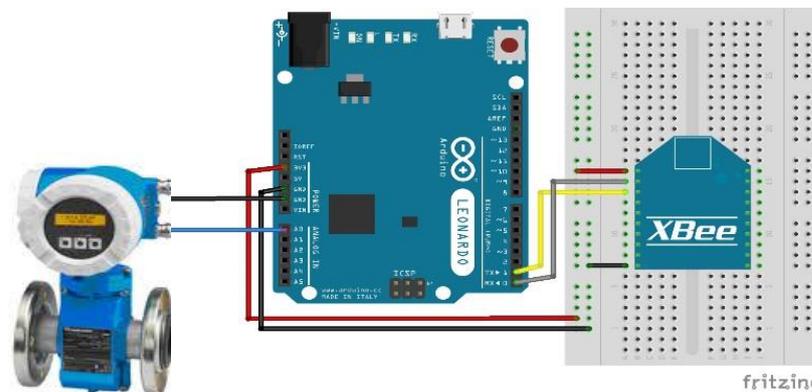
Variável	Princípio	Protocolo
Pressão (gás e líquido)	Capacitivo e silício ressonante	Analógica, Foundation Fieldbus, Profibus, Wi-Fi e Hart
Nível	Diferencial de pressão, capacitivo (eletrodo e placa) e borbulhamento	Analógica, Foundation Fieldbus, Profibus e ASI3,
Vazão (gás e líquido)	Magnético, Ultrassom, placa de orifício, orifício integral e coriolis	Analógica, DeviceNet e Profibus
Temperatura	Termoresistência e termopar	Analógica, Foundation Fieldbus e Profibus
pH	Diferença de potencial	Analógica
Oxigênio dissolvido	Diferença de potencial com membrana	Analógica

Fonte: Autoria própria

Além dos recursos informados acima, entre os CLPs do processo, há uma comunicação Modbus com um outro CLP que irá inserir defeitos programados com a finalidade de analisar os efeitos e propor soluções.

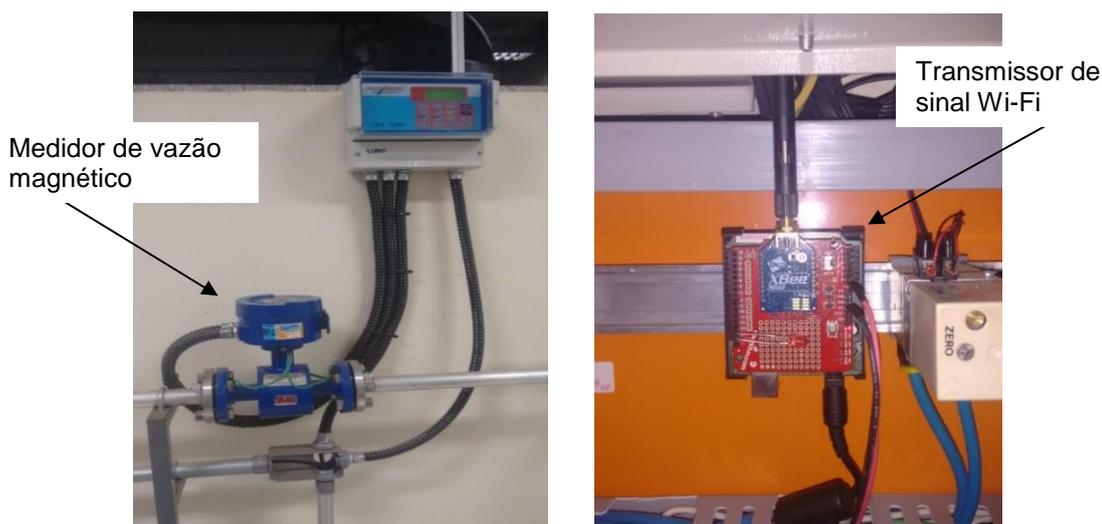
A malha de controle onde foram concentrados os estudos é composta por um medidor de vazão magnético da marca Contech com a unidade eletrônica remota. A unidade eletrônica, foi configurada para uma escala de vazão de 0 a 5 m<sup>3</sup>/h e um sinal analógico proporcional de 0 a 10Vcc. Este sinal analógico é enviado a uma plataforma Arduino onde este valor analógico será encapsulado no Modbus e por sua vez entrará na camada de aplicação do modelo ISO/OSI que será transmitida pelo Wi-Fi a uma taxa de 2 segundos. Para simplificar, podemos dizer que será realizada a conversão de um sinal analógico para Ethernet TCP/IP Wi-Fi. A ligação entre os componentes está representada na Figura 21 e a instalação é apresentada na Figura 21.

Figura 21: Ligação elétrica do medidor de vazão magnético e transmissor de rede Wi-Fi



Fonte: Autoria própria

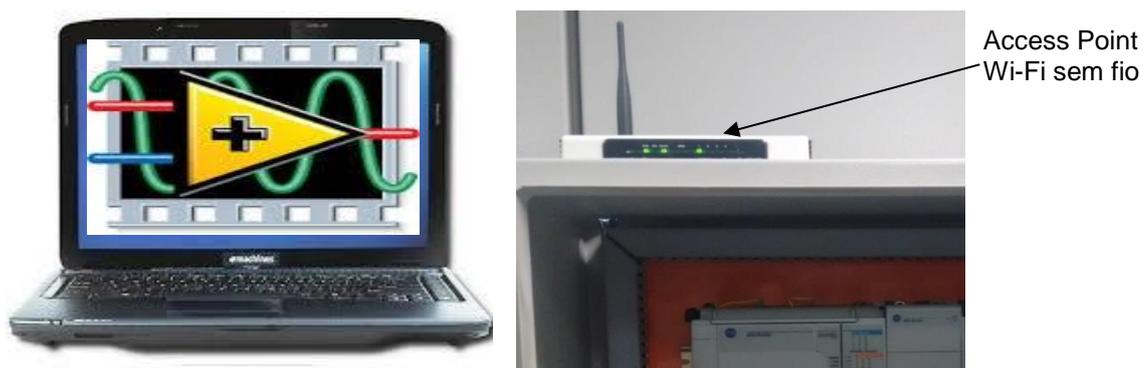
Figura 22: Instalação do medidor de vazão magnético e transmissor de rede Wi-Fi



Fonte: Autoria própria

Na Figura 23, um Notebook com LabVIEW (controlador) coletará o sinal do transmissor em um *Access Point* e fará a tratamento da mensagem com a finalidade de separar o valor da vazão para poder realizar os cálculos de controle que serão enviados novamente ao *Access Point*. Para o cálculo do sinal de controle, foram implementados um controlador PID tradicional e um PIDPlus.

Figura 23: Coleta das informações de vazão e processamento.



Fonte: Autoria própria

A separação do valor da vazão é realizada através dos blocos de funções Modbus do LabVIEW da Figura 24, onde também foi tratado para um valor de unidade de engenharia para que o controlador consiga realizar o controle de forma eficiente.

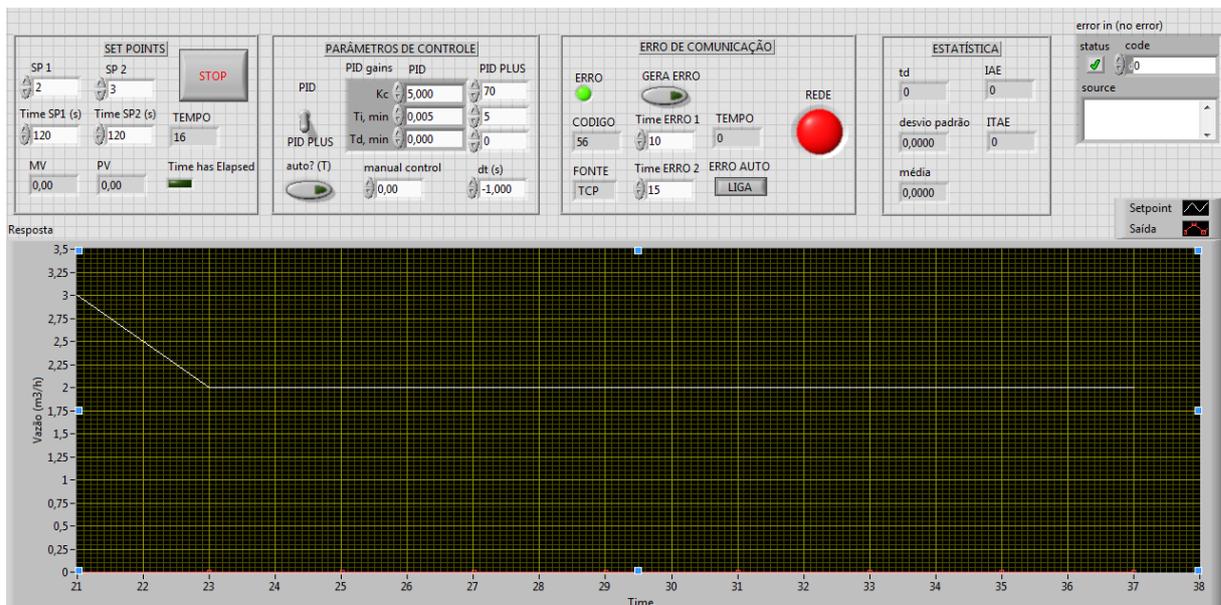
Figura 24: Blocos de funções Modbus.



Fonte: Software LabVIEW

Depois de tratado e padronizado, este sinal que é utilizado para o controle. Junto com os valores de saída do controlador e set point, são registrados em formato de gráfico como o da Figura 25 e armazenados para posterior análise.

Figura 25: Tela gráfica dos comandos e das variáveis do controle.



Fonte: Autoria própria

O sinal de controle é transmitido através de uma rede Ethernet TCP/IP com fio entre o *Access Point* e uma plataforma Arduino que fará a separação do dado da saída de controle e irá converter, através de código, em um sinal analógico de 0 a 5Vcc que será enviado a um inversor de frequência. A ligação elétrica é representada na Figura 26 e sua instalação na Figura 27 que fará o controle de velocidade de uma moto-bomba que por sua vez irá controlar a vazão.

Figura 26: Ligação elétrica entre Arduino e Inversor de Frequência.



Fonte: Autoria própria

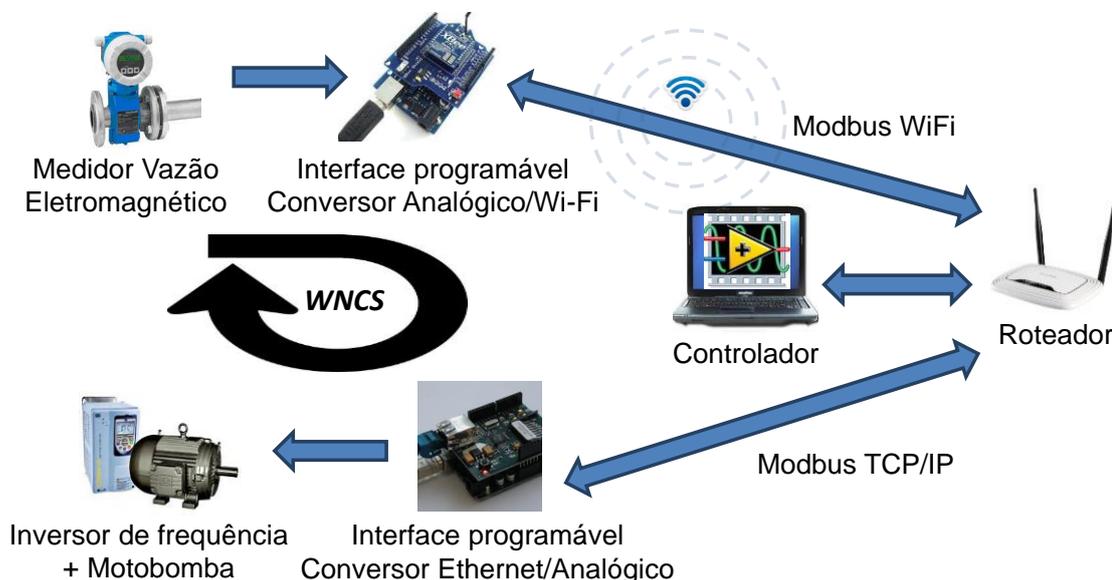
Figura 27: Instalação do Arduino e Inversor de Frequência



Fonte: Autoria própria

Para um melhor entendimento de todo processo de transmissão e controle da malha de controle de vazão, o esquemático do WNCS pode ser visto na Figura 28.

Figura 28: Arquitetura do WNCS com redes Modbus



Fonte: Autoria própria

#### 4.3 ESTRATÉGIA DE CONTROLE

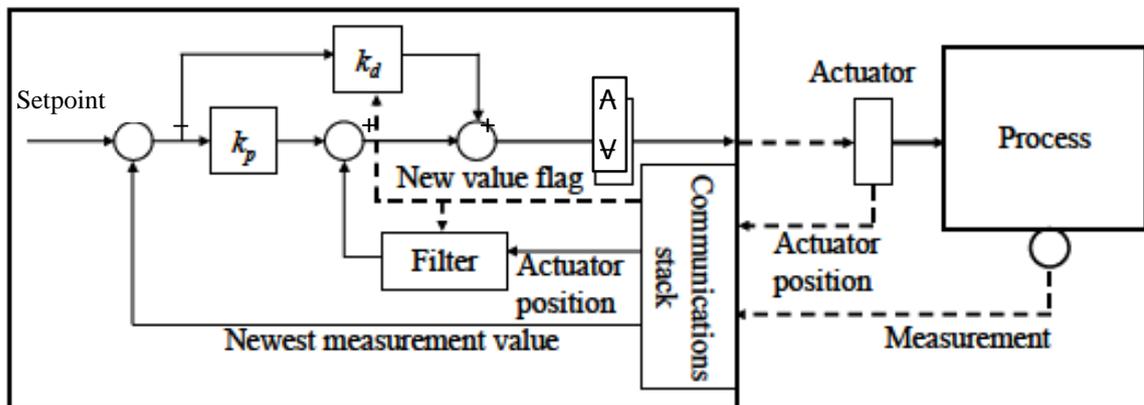
Um pressuposto em controle de processo sempre foi que sua execução se dará em uma base periódica e que um novo valor de medição está disponível para cada execução. No entanto, para minimizar o consumo de energia de um transmissor sem fio, os valores de medição podem ser transmitidos com uma baixa frequência, e somente se o valor da medição mudar significativamente (BLEVINS et al., 2014). Desta forma o controle tem que ser modificado para poder trabalhar com as atualizações de medições não periódicas. Além disso, é importante que a perda de comunicação seja tratada automaticamente pelo controle de uma forma a não introduzir uma interrupção do processo.

Quando a medição não é atualizada em uma base periódica, um PID tradicional não é indicado, pois as ações de controle não serão calculadas de forma correta. Como o controle só é executado quando uma nova medida é informada, isso poderia resultar em um atraso na resposta de um controlador, portanto é preciso modificá-lo. Para tornar esta tecnologia de WNCS mais confiável, muitas técnicas de controle têm sido pesquisadas (BLEVINS et al., 2014) como o PID com Preditor de Smith, PID com Filtro de Kalman e também o PIDplus que representa uma modificação do conhecido algoritmo PID. A chave para se compreender como

o PID deve ser modificado é realizando o reset do PID implementado utilizando uma rede de realimentação e um filtro onde a constante de tempo é um reflexo direto da resposta dinâmica do processo. Com base neste entendimento, o cálculo de reposição do PID é modificado para controle sem fios.

Um exemplo de PID modificado é o PIDPlus do sistema de controle DeltaV da *Emerson Process* para controle em malha fechada, usando um transmissor de rede sem fio. A implementação PIDPlus de Song et al., (2006) é ilustrada na Figura 29. O PIDPlus mantém o sinal de controle no último nível calculado até que uma nova medida seja recebida. Por fim é importante notar que sua sintonia é independente do período de amostragem, depende apenas das características físicas da planta.

Figura 29: Estrutura do controlador PIDPlus



Fonte: Song et al. (2006)

A realimentação (*newest measurement value*) e o filtro de 1ª ordem (*filter*) são modificados para criar a contribuição de reposição com o seguinte comportamento:

- manter a última saída do filtro calculado ( $F_{N-1}$ ), até uma nova medição ser informada (*new value flag*);
- quando uma nova medição é recebida (*new value flag*), utilize a nova saída do filtro como realimentação ( $F_N$ ).

Uma diferença do PID e PIDPLUS está na parte integrativa que foi substituído por um filtro de 1ª ordem. A saída do filtro é calculada da seguinte forma (1):

$$F_N = F_{N-1} + (O_{N-1} - F_{N-1}) \left(1 - e^{\frac{-\Delta T}{T_{reset}}}\right) \quad (1)$$

$F_N$  = nova saída do filtro;

$F_{N-1}$  = saída do filtro na última execução;

$O_{N-1}$  = saída do controlador na última execução;

$\Delta T$  = intervalo de tempo desde que o último valor medido foi recebido;

$T_{reset}$  = constante de tempo da planta somado ao tempo morto. O tempo integrativo ( $T_i$ ) do controlador também pode ser usado como um parâmetro RESET simplificado

A parte derivativa é substituída da seguinte forma (2):

$$O_D = K_D \frac{e_N - e_{N-1}}{\Delta T} \quad (2)$$

$e_N$  = erro atual;

$e_{N-1}$  = último erro;

$\Delta T$  = intervalo de tempo desde que o último valor medido foi recebido;

$O_D$  = termo derivativo do controlador;

$K_D$  = ganho derivativo.

Considere a contribuição da parte derivativa quando as entradas são perdidas durante vários períodos. Para o algoritmo PID tradicional, o divisor na parte derivativa seria o período (discretização do controlador), enquanto que, no novo algoritmo PIDPlus é o tempo decorrido entre duas medições recebidas com sucesso ( $\Delta T$ ). É óbvio que o algoritmo modificado produz uma ação derivativa menor do que o algoritmo de controle PID.

Na implementação do PIDPLUS, o cálculo de reposição compensa automaticamente a alteração da medição e taxa de atualização da medição. Os cálculos do termo derivativo para um novo valor de medição não estão disponíveis a cada execução do PID. Assim, não há necessidade de modificar a sincronização para o controle sem fio, ou seja, o ajuste é baseado estritamente no ganho e dinâmica do processo.

## 5. RESULTADOS E DISCUSSÕES

### 5.1 MÉTRICAS DE DESEMPENHO DO MODBUS WI-FI

Os principais parâmetros relacionados ao desempenho de WNCS são o atraso de comunicação, *jitter* e a perda de mensagens transmitidas. O mais crítico destas métricas é o tempo que decorre entre o envio de um dado de um nó até o outro recebê-lo, ou o tempo de atraso ou atraso de comunicação (ANAND et al., 2009). Grandes desvios imprevisíveis do tempo de atraso afetam significativamente o desempenho de um WNCS e torna-se impossível calcular um intervalo de pacotes confiável ou a taxa de amostragem para o sistema.

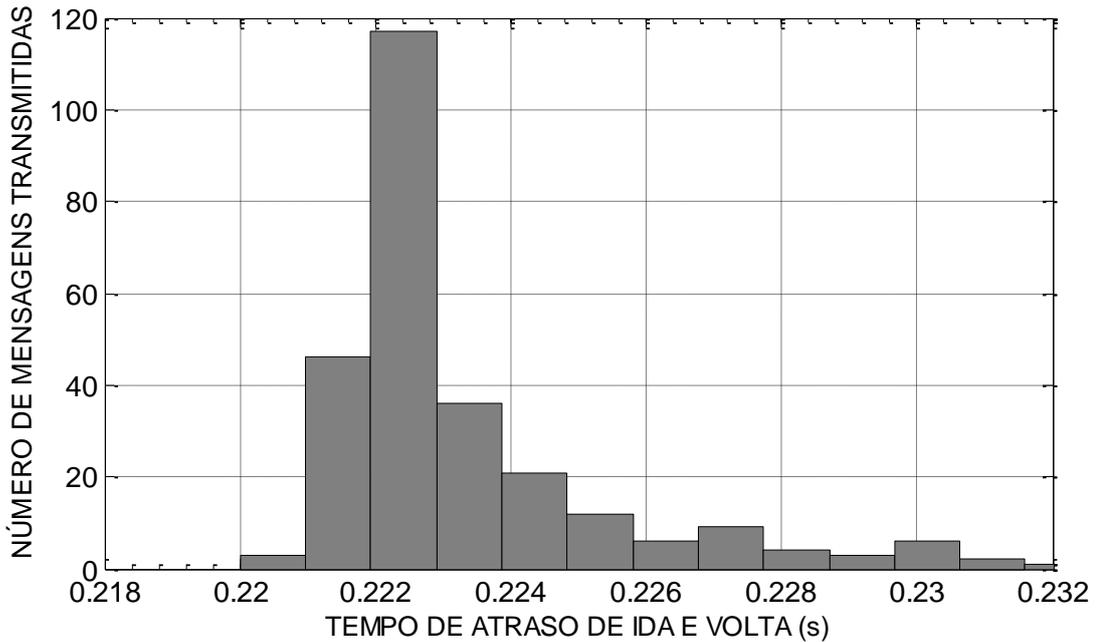
A taxa de utilização da rede é a razão entre a capacidade efetiva de transmissão de dados e a capacidade momentânea usada por uma comunicação. A utilização da rede pode ser definida como a percentagem de tempo durante o qual o meio de transmissão é ocupado. A alta utilização da rede pode aumentar o tempo médio de atraso e o *jitter*, e conseqüentemente impactar o desempenho do WNCS.

Na maioria das aplicações de sistema de controle via rede, é necessário que todos os dados sejam transmitidos com êxito. É, portanto, importante avaliar um protocolo de acordo com o número ou a possibilidade de mensagens não enviadas. Retransmissões podem reduzir ou eliminar este problema, mas irá aumentar significativamente o *jitter* e atraso médio.

Neste trabalho foram analisadas as duas principais métricas de desempenho de rede relacionadas ao controle em rede, que são o tempo de atraso de comunicação (Td) e *jitter* (J). Uma maneira de medir esse tempo de atraso é medir o tempo de comunicação de ida e volta dentro da malha. O tempo de viagem é o tempo de atraso no envio de um pacote de um nó para outro e vice-versa. Se um cálculo estatístico é realizado a partir de uma quantidade de atrasos, podemos obter o tempo de atraso médio das transmissões de mensagens na rede sem fio. Calculando o desvio padrão de um conjunto de atrasos nos dá uma medida da sensibilidade de condições de rede ideais. Na maioria dos casos, o desvio padrão dos tempos de atraso é um bom indicador do *jitter*.

A Figura 30 tem-se uma distribuição dos tempos de atraso obtidos com o envio de mensagens no Modbus Wi-Fi. Esta análise considerou o cálculo do tempo com os hardwares (microcontrolador, rádio e etc.) utilizados na implementação deste trabalho. A variabilidade nos valores de medição do tempo de atraso fornece o *jitter* do WNCS.

Figura 30: Histograma do tempo de atraso da rede Modbus Wi-Fi



Fonte: Autoria própria

Como pode ser observado Figura 30, a maioria dos valores aproxima-se do valor médio de 0,2226s. Sem a presença de grandes valores extremos, o histograma nos mostra um bom determinismo, como é possível observar na Tabela 4.

Tabela 4: Desempenho da rede sem fio no controle PID.

Controle	Td (ms)	J (ms)	Pior valor (ms)	Mensagem Perdida
PID	222,6	10,7	231	0

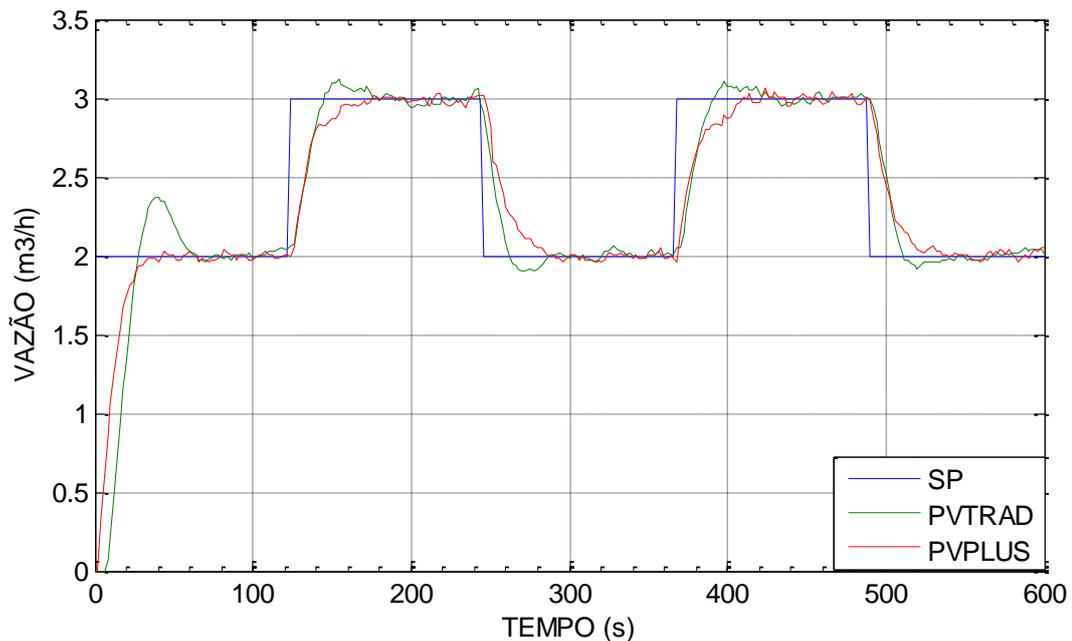
Fonte: Autoria própria

## 5.2 COMPARAÇÃO DE CONTROLADORES

Nesta etapa do trabalho, buscou-se comparar e avaliar o desempenho de controle do WNCS operando com o controlador PID tradicional e com o PIDPlus. Os controladores PID e PIDPlus foram submetidos às mesmas condições de operação e submetidos a distúrbios de mudança de *setpoint* e perda de comunicação para que as respostas possam ser analisadas de forma qualitativa e quantitativa.

O comportamento dos dois controladores para a malha de vazão proposto em situações normais, ou seja, quando a transmissão de dados sem fio está sendo realizada de forma eficiente e sem interferências ou erros, somente variação de *setpoint* para podermos comparar o desempenho. Conforme mostrado na Figura 31, os desempenhos de controle do WNCS numa situação ideal numa operação livre de falhas de comunicação são semelhantes para o controlador PID e PIDPlus.

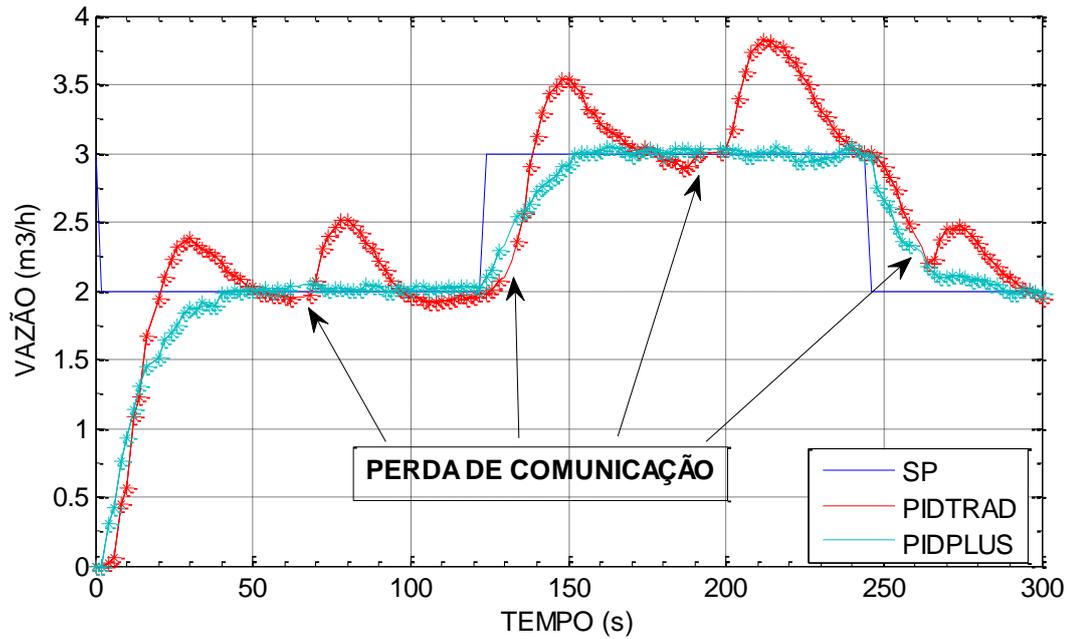
Figura 31: Controle de vazão utilizando o PID e PIDPlus



Fonte: Autoria própria

Na Figura 32, o processo foi submetido ao mesmo perfil de trabalho da análise anterior, mas com o acréscimo de momentos de falhas na comunicação, onde a cada 60 segundos de transmissão, foi simulado 6 segundos de perda de mensagens do sensor de vazão, gerada por um erro programado no software de aquisição de dados a uma taxa de atualização de 2 segundos. Podemos observar que o PID tradicional se desestabilizou pelo fato do controlador não se adequar a ausência do valor da vazão, ocasionando a saturação da saída do controlador e conseqüentemente um desgaste excessivo no elemento final de controle. Em um processo industrial, essa situação seria prejudicial e deveria ser evitada.

Figura 32: Controle de vazão: PID e PIDPlus com falhas de comunicação



Fonte: Autoria própria

Analisando a Figura 32 observa-se que o controlador PIDPlus conseguiu manter o processo estável mesmo na ausência do valor da vazão. O controlador PIDPlus mantém o último valor da saída do controlador (sinal de controle), pois ele calcula as contribuições do termo integral e derivativo para a saída do controlador somente quando há uma atualização da medição da variável e usa o tempo decorrido entre as atualizações em seus cálculos.

Assim, o PIDPlus atua apenas quando é recebido um novo valor da medição e considera que a mudança observada na variável medida ocorreu não apenas no último período de execução do controlador, mas ao longo do tempo decorrido entre as atualizações. Dessa forma, quando há uma perda de comunicação com o transmissor ou elemento final de controle, o PIDPlus não fornece outra ação de reposição, ele aguarda novas atualizações. Quando a comunicação é restabelecida, ele atua sobre a nova atualização.

Para analisar o desempenho dos dois controladores, foram utilizados os índices de desempenho IAE (Integral Absoluta do Erro) e ITAE (Integral do Erros Absoluto multiplicado pelo Tempo), onde seu desempenho sem falhas e depois inserindo falhas na comunicação foi comparado. Na Tabela 5, podemos comprovar que o desempenho de controle do PIDPlus para o WNCs operando sob falhas na transmissão do sinal de vazão é melhor que o PID tradicional.

Tabela 5: Desempenho dos controladores PID e PIDPlus.

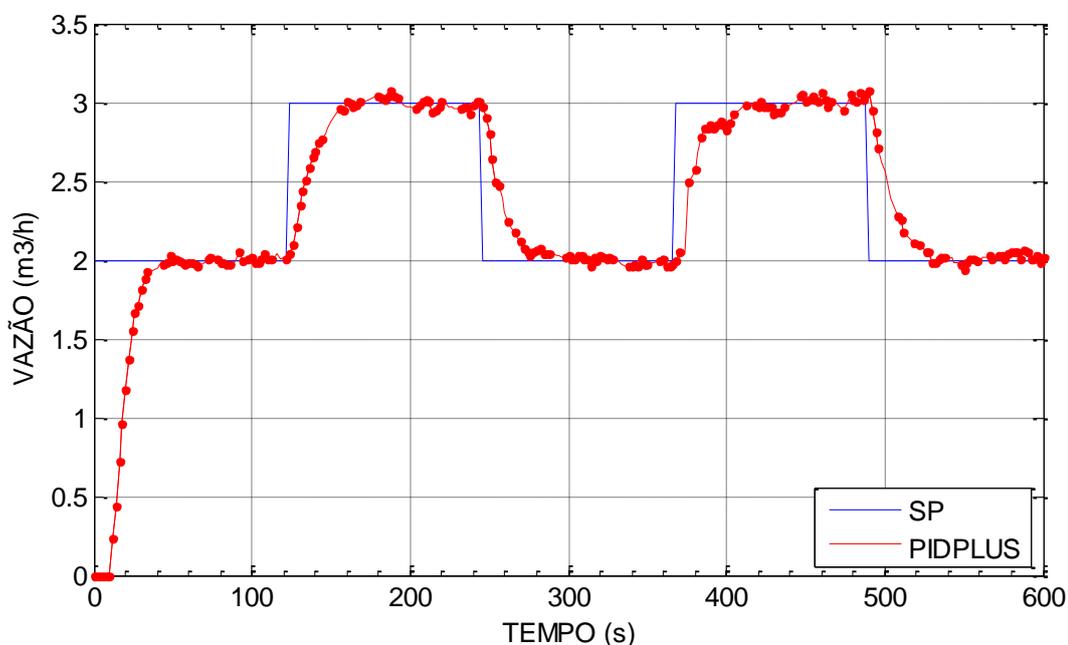
Índice de Desempenho	Controle			
	PID Trad.	PIDPlus	PID Trad. + Falha	PIDPlus + Falha
IAE	55	41	91	43
ITAE	10701	9259	24291	9355

Fonte: Autoria própria

### 5.3 DESEMPENHO DO WNCs SOB CONDIÇÕES DE FALHAS DE COMUNICAÇÃO DE FORMA ALEATÓRIA E SEQUENCIAL

Nesta etapa os testes de controle foram realizados inserindo falhas de comunicação de forma aleatória e também sequencial. Para os testes com falhas aleatórias, o controlador foi configurado para que as falhas de comunicação variassem de 2 a 10 segundos de forma randômica e acontecesse a qualquer momento em que o processo estivesse sendo controlado, também de forma randômica. Na Figura 33 pode-se observar as falhas de comunicação na linha da variável do processo onde não há marcadores.

Figura 33: Controle de vazão: PIDPlus com falhas de comunicação aleatória



Fonte: Autoria própria

Pode-se observar através da Tabela 6 que mesmo inserindo falhas de comunicação na rede, o controlador consegue se manter com índices de desempenho bem parecido com o controle sem falhas.

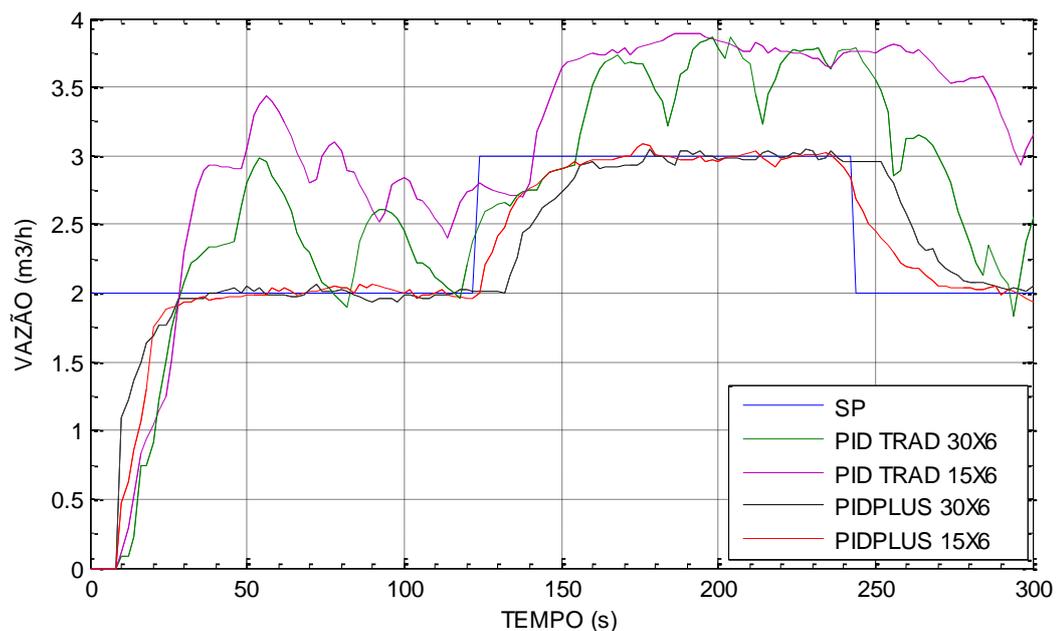
Tabela 6: Desempenho do controlador PIDPlus com falhas de comunicação aleatória

Índice de Desempenho	Controle	
	PIDPlus	PIDPlus + Falha
IAE	41	43
ITAE	9259	9355

Fonte: Autoria própria

Para verificar a robustez do WNCS com o PIDPlus, foram realizados testes adicionais entre o PIDPLUS e o PID tradicional, obedecendo o mesmo perfil de distúrbios e com uma maior frequência de falhas de comunicação: 30 s de operação e 6 s com falha na comunicação (30x6) e com 15 s de operação e 6 s com falha (15x6). Lembrando que o período de amostragem é de 2 s, portanto três mensagens são perdidas. Os resultados dessa comparação são mostrados na Figura 34.

Figura 34: Controle de vazão: PIDPlus e PID tradicional com falhas de comunicação sequencial 30x6 e 15x6



Fonte: Autoria própria

Na Figura 34, é possível verificar notória degradação no desempenho de controle com o PID tradicional, ocasionando uma resposta muito oscilatória, já que o tempo (entre falhas) que o controlador tinha para se ajustar diminuiu. Este controlador nestas condições não poderia ser utilizado neste processo. Em contrapartida, o PIDPlus obteve desempenho melhor, controlando o WNCS adequadamente.

Na Tabela 7, comprova-se essa robustez com os índices de desempenho observamos que o controle do PIDPLUS se manteve estável mesmo com as falhas inseridas, mas o PID tradicional não conseguiu realizar o controle mediante as falhas de comunicação.

Tabela 7: Desempenho dos controladores com falhas de comunicação sequencial 30x6 e 15x6

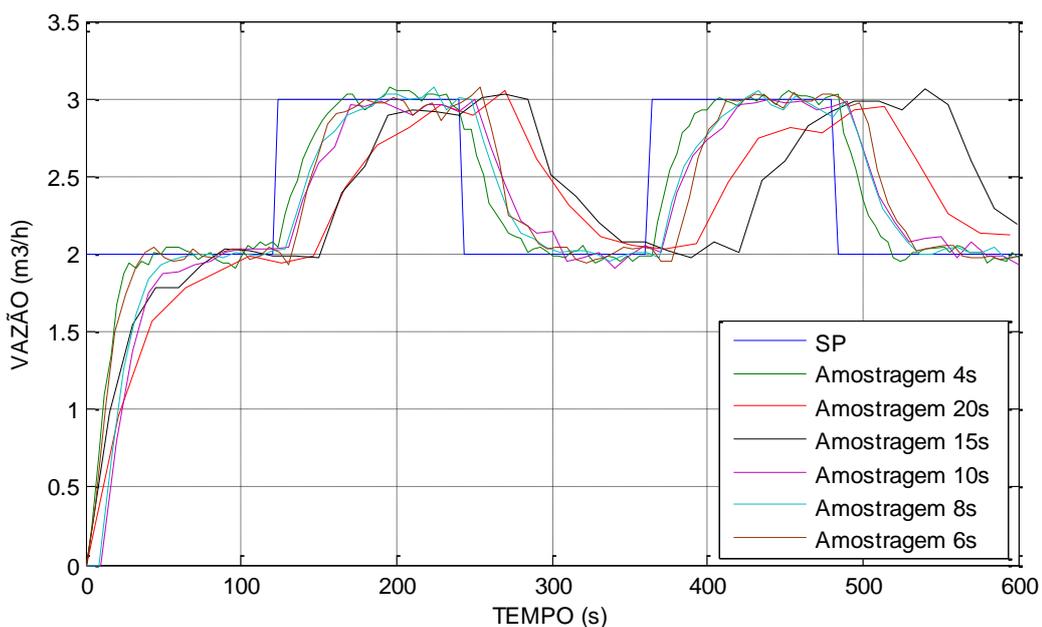
Índice de Desempenho	Controle			
	PID Trad.	PIDPlus	PID Trad. + Falha	PIDPlus + Falha
<b>IAE 30X6</b>	55	41	334	42
<b>ITAE 30X6</b>	10701	9259	100309	8949
<b>IAE 15X6</b>	55	41	449	43
<b>ITAE 15X6</b>	10701	9259	136312	8168

Fonte: Autoria própria

#### 5.4 DESEMPENHO DO WNCS SOB VARIAÇÃO DO PERÍODO DE AMOSTRAGEM DO SENSOR SEM FIO

Para todos os experimentos anteriores, o controlador do WNCS estava operando com um período de amostragem do sensor sem fio (intervalo entre transmissões de mensagem da variável controlada) de 2 segundos. Em WNCS, esse é dos principais parâmetros que podem influenciar o desempenho de controle do sistema, além de ser um parâmetro diretamente relacionado ao consumo energético do sensor sem fio (MANSANO et al., 2014). Do ponto de vista energético, do desempenho de controle, melhor para o WNCS. Dessa forma, é importante conhecer a influência da variação deste parâmetro no desempenho do WNCS e o período de amostragem limite para obtenção de um desempenho aceitável para o WNCS operando com o PIDPlus. Para a realização destas análises, o período de amostragem do sensor sem fio, foi variado de 4 até 20 s. A comparação das respostas do WNCS é mostrada Figura 35.

Figura 35: WNCS de vazão: Impacto do período de amostragem do sensor sem fio na resposta



Fonte: Autoria própria

Nota-se na Tabela 8 Figura 35 que para alterações do período de amostragem de até 10 s, o controlador PIDPlus conseguiu manter uma resposta adequada ao perfil do *setpoint*. No entanto, para valores acima de 10 s, o controle apresenta queda de desempenho, sendo este o período de amostragem limite para obtenção de um desempenho aceitável para o WNCS. Essa é uma constatação importante pois ao contrário do PIDPlus, o PID tradicional, que é discretizado e sintonizado para um período de amostragem específico (2s) tem seu desempenho degradado (ANDRADE et al., 2016). Isso confirma uma das características do PIDPlus: não é necessária uma nova sintonização dos ganhos do controlador PIDPlus, ou seja, o controlador PIDPlus pode ser projetado a partir do PID tradicional.

Tabela 8: Desempenho do WNCS variando o período de amostragem do sensor sem fio

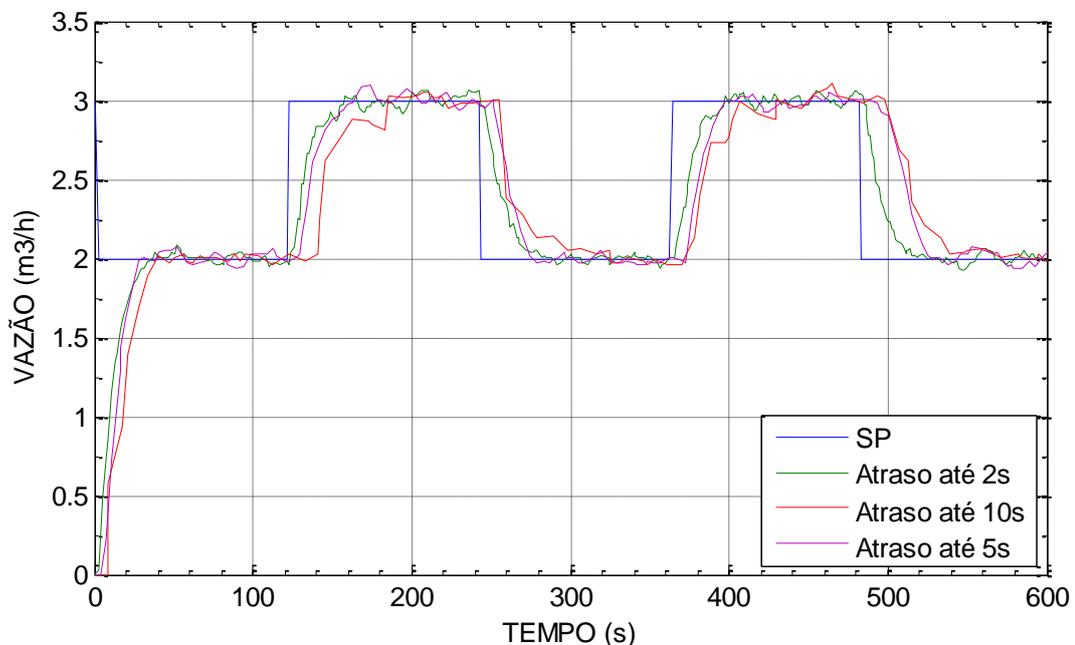
Índice de Desempenho	Controle PIDPlus						
	2 s	4 s	6 s	8 s	10 s	15s	20 s
<b>IAE (MEDIA)</b>	0,18	0,22	0,26	0,33	0,37	0,38	0,51

Fonte: Autoria própria

## 5.5 DESEMPENHO DO WNCS SOB VARIAÇÃO DO ATRASO DE COMUNICAÇÃO

O último parâmetro analisado em relação ao seu impacto no desempenho de controle do WNCS desenvolvido foi o atraso de comunicação (*delay*). Em WNCS, o atraso de comunicação total (atraso do sensor - controlador + atraso controlador - atuador) geralmente é variável no tempo. Para a realização desta análise, foi inserido no loop de controle do WNCS um intervalo de tempo randômico, de forma a representar a característica variável de um atraso de comunicação. Esse atraso foi variado aleatoriamente em três casos diferentes: atraso de até 2, até 5 e até 10 s. A comparação das respostas do WNCS é mostrada na Figura 36.

Figura 36: Controle de vazão: PIDPlus com atraso de comunicação variável



Fonte: Autoria própria

Os resultados na Figura 36 mostram que o controlador PIDPlus consegue operar adequadamente na presença de atrasos variantes no tempo. Nos testes realizados com diferentes valores de atrasos de comunicação inseridos na malha de controle fechado, o desempenho do WNCS se manteve próximo ao ideal (caso inicial onde não foi inserido atraso adicional).

## 6. CONCLUSÃO

Os resultados demonstram que a implementação em hardware dedicado do protocolo industrial Modbus para a comunicação via TCP/IP e Wi-Fi foram efetivas, permitindo adaptar instrumentos analógicos em dispositivos Modbus compatível e transmitir sinais de controle e realimentação. Testes de operação do WNCS demonstraram a confiabilidade na comunicação via Modbus implementada, obtendo baixo *jitter* na transmissão de mensagens e baixo índice de perda de mensagens transmitidas.

A implementação do protocolo Modbus foi detalhadamente descrita, gerando um material de referência (fluxograma) para orientar outras implementações do Modbus em sistemas embarcados. Além disso, o código gerado pela implementação da camada de aplicação do Modbus na plataforma Arduino (*Sketch*) permite reuso em outras plataformas de hardware embarcado, que são compatíveis com a linguagem de programação do Arduino, tornando-as compatíveis com aplicações Modbus.

O controlador PIDPlus atende ao controle de processos via rede que utilizam transmissores com e sem fio, mostrando-se com melhor robustez e desempenho superior ao PID tradicional nos casos estudados de perda de dados transmitidos, presença de atrasos de comunicação variantes no tempo e alteração o período de amostragem do sensor sem fio. No caso de perda de dados transmitidos ou falhas de comunicação, o PIDPlus foi capaz de manter desempenho equiparável ao caso ideal (sem falhas) para os casos de falhas sequenciais e aleatórias. Também se constatou que controlador PIDPlus opera adequadamente em uma faixa de período de amostragem que inclui a frequência de sintonia do PID tradicional e períodos de amostragem variáveis, com a vantagem de não requerer nova sintonia do controlador.

Adicionalmente, o uso do controlador PIDPlus para controle via rede sem fio é fortemente recomendado nas seguintes situações:

- o tempo de atualização da malha de controle fechado é maior do que o tempo de resposta do processo;
- aplicações com maior probabilidade de ocorrência de erros e falhas de atualização na rede sem fio;
- elemento final de controle apresenta significativa manutenção em função de acionamentos rápidos e bruscos, fazem com que o equipamento trabalhe em seu limite projetado.

## 7. REFERÊNCIAS

AAKVAAG, N., M. MATHIESEN, THONET, G. Timing and Power Issues in Wireless Sensor Networks – an Industrial Test Case. In: **Proceedings of the 2005 International Conference on Parallel Processing Workshops**, p. 419-426

ALFA INSTRUMENTOS. **Protocolo de Comunicação Modbus RTU/ASCII**, Alfa Instrumentos, 2000.

ANAND D. M., MOYNE J. R., TILBURY, D. M. Performance evaluation of wireless networks for factory automation applications. in: **Proc. Of the 5th Annual IEEE Conf. on Automation Science and Engineering (CASE)**, Bangalore, India, p. 340-346, Ago. 2009

ANDRADE, Y. S.; MANSANO, R. K.; GODOY, E. P. Projeto de Controle Não Periódico para Sistemas de Controle Via Redes Sem Fio. In: **Congresso Brasileiro de Automática (CBA)**, 2016.

BAILLIEUL, J.; ANTSAKLIS, P. J. Control and Communication Challenges in Networked Real Time Systems. **Proceedings of IEEE Technology of Networked Control Systems**, v. 95, p. 09-28, 2007.

BLEVINS, T; NIXON, M; WOJSZNIS, W. **PID Control Using Wireless Measurements American Control Conference (ACC)**, p. 1-6 Jun. 2014..

CLOOSTERMAN, M. B. G.; VAN DE WOUW, N.; HEEMELS, W. P. M. H.; NIJMEIJER, H. Stability of networked control systems with uncertain time-varying delays. **IEEE Transactions on Automatic Control**, v. 54, n. 7, p. 1575–1580, jul. 2009.

DZUNG, D.; APNESETH, C.; ENDERSEN, J.; FREY, J. E. Design and Implementation of a Real-Time Wireless Sensor/Actuator Communication System. In: **10th IEEE Conference on, Emerging Technologies and Factory Automation**, 2005, p. 443-442.

EMERSON. Emerson Process 2006. **Wi-Fi Networks**. Disponível em: [http://plantweb.emersonprocess.com/university/Library\\_Downloadable\\_Courses.asp#wir](http://plantweb.emersonprocess.com/university/Library_Downloadable_Courses.asp#wir)  
Acesso em: 30 out 2007.

FISCHIONE, C.; PARK, P.; DI MARCO, P.; JOHANSSON, K. H. Design Principles of Wireless Sensor Networks Protocols for Control Applications. S.K. Mazumder (Ed.). **Wireless Networking Based Control**, 2011, Ch. 9, Springer, pp. 203-238.

GALLOWAY, B.; HANCKE, G. P. Introduction to Industrial Control Networks. **IEEE Communications Surveys & Tutorials**. 2013, v.15, p. 860-880.

GODOY E. P.; OLIVEIRA T. A.; SCORZONI F.; PORTO A. J. V. Leveraging Wireless Devices for Networked Control Systems in Industrial Applications. **Brazilian Journal of Instrumentation and Control**, v. 1, p. 21-28, 2013.

GODOY E. P.; SOUSA R. V.; PORTO A. J. V.; INAMASU R.Y. Design of CAN-Based Distributed Control Systems with Optimized Configuration, **Journal of the Brazilian Society of Mechanical Sciences and Engineering**, v. 32, n. 4 , p. 420-426, 2010.

- GUPTA, R. A. ; CHOW, M. Y. Networked Control System: Overview and Research Trends. **IEEE Transactions on Industrial Electronics**, 2010, v. 57, n. 7, p. 2527-2535.
- HEEMELS, W. P. M. H.; TEEL A. R.; VAN DE WOUW N.; DRAGAN, N. Networked Control Systems With Communication Constraints: Tradeoffs Between Transmission Intervals, Delays and Performance. **IEEE Transactions on Automatic Control**, 2010, v. 55, n. 8, p. 1781-1796.
- HESPANHA J. P, NAGHSHTABRIZI P.; XU Y. A Survey of Recent Results in Networked Control Systems, **IEEE Technology of Networked Control Systems**, Vol. 95, No. 1, pp. 138-162, 2007.
- ISA-SP100.11 (2006). Call for Proposal: **Wireless for Industrial Process Measurement and Control**. Disponível em [http://www.isa.org/filestore/ISASP100\\_11\\_CFP\\_14Jul06\\_Final.pdf](http://www.isa.org/filestore/ISASP100_11_CFP_14Jul06_Final.pdf) Acesso em 30 out 2007.
- LOW, K. S.; WIN, W. N. N.; MENG, J.E. Wireless Sensor Networks for Industrial Environments. In: **International Conference on Computational Modelling, Control and Automation, 2005 and International Conference on Intelligent Agents, Web Technologies, and Internet Commerce**, 2005, 2, p. 271-276.
- MANSANO, R. K.; GODOY, E. P. AND PORTO, A. J. V. The Benefits of Soft Sensor and Multi-rate Control for the Implementation of Wireless Networked Control Systems. **Sensors**. 2014, p. 24441-24461.
- MILLAN, Y. A.; VARGAS, F.; MOLANO, F. AND MOJICA, E. A Wireless Networked Control Systems Review- **IEEE IX Latin American and IEEE Colombian Conference on Automatic Control and Industry Applications (LARC)**, 2011.
- MODBUS (2015). **Modbus Organization**. Disponível em: <<http://www.modbus.org/>> Acesso em 10 dez 2015.
- MOYNE J. R.; TILBURY, D.M. The Emergence of Industrial Control Networks for Manufacturing Control, Diagnostics, and Safety Data. **IEEE Technology of Networked Control Systems**, v. 95, p. 29-47, 2007.
- NAGHSHTABRIZI, P.; HESPANHA, J. P. Implementation Considerations For Wireless Networked Control Systems, S.K.Mazumder (ed.), **Wireless Networking Based Control**, 2011, Ch. 1, Springer, p. 1-27.
- PAAVOLA, M. LEIVISKA, K. Wireless Sensor Networks in Industrial Automation, J.S. Blanes (Ed.). **Factory Automation**, 2010, Ch 10, Intech, p. 201-220.
- Petersen, S. and Carlsen, S. Wireless HART Versus ISA100.11a: The Format War Hits the Factory Floor. **IEEE Industrial Electronics Magazine**, 2011, Vol. 5, No. 4, p. 23-34.
- PIGGIN R.; BRANDT D. **Wireless Ethernet for industrial applications**. **Assembly Automation**, v. 26, 2006.

SADI, Y.; ERGEN, S. C.; PANGUN, P. Minimum Energy Data Transmission for Wireless Networked Control Systems, **IEEE Transactions on Wireless Communications**, v. 13, n. 4, p. 2163-2175, 2014.

SAUTER, T. The Three Generations of Field-Level Networks—Evolution and Compatibility Issues, **IEEE Transactions on Industrial Electronics**, v. 57, n. 11, p. 3585-3595, Nov. 2010

SEIXAS, Constantino. **Protocolos Orientados a Caracter**. UFMG – Departamento de Engenharia Eletrônica, Minas Gerais, 2009.

SONG, J. et. al. **Improving PID control with unreliable communications**. In ISA EXPO Technical Conference 2006.

THOMESSE, J. P. Fieldbuses and interoperability. **Control Engineering Practice**, v. 7, n. 1, p. 81–94, 1999.